Tampereen yliopisto

Marika Ristolainen

TIETOTURVAN JALKAUTTAMINEN ENERGIAYHTIÖSSÄ

Tekniikan ja luonnontieteiden tiedekunta
Diplomityö
Huhtikuu 2020

TIIVISTELMÄ

Marika Ristolainen: Tietoturvan jalkauttaminen energiayhtiössä

Tampereen Yliopisto

Johtamisen ja tietotekniikan tutkinto-ohjelma

Tarkastajat: professori Marko Seppänen ja yliopistonlehtori Rainer Breite

Diplomityö

Huhtikuu 2020

Tietoturvallisuusasiat ovat nousseet energiayhtiöiden suurimpiin huolenaiheisiin viimeisten vuosikymmenien aikana. Tietojenkalastelua ja huijausviestejä vastaanotetaan jatkuvasti etenkin kohdistuen Office365 -tuotteisiin. Pelkästään erilaisia käyttäjiin ja sitä kautta kohdeyrityksen työntekijöihin kohdistuvia huijauspuheluita saatiin käsiteltyä Suomessa helmikuussa 2020 reilu 1300 kpl, todellisten huijauspuhelumäärien ollessa oletettavasti huomattavasti korkeampi. Pelkästään edellä mainitut seikat puoltavat tietoturvakulttuurin kehittämistä ja erityisesti yrityksen henkilökunnan huolellista jatkuvaa perehdyttämistä taistelussa tietoturvarikollisuutta vastaan.

Tutkimuksen aiheena oli energiayhtiön tietoturvakulttuurin kehittäminen. Aihetta rajattiin työn alkuvaiheessa siten, että se keskittyy tietoturvaperehdytyksen jalkautuksen kehittämiseen ja soveltuvan perehdytystavan valintaan. Työssä pyritään vastaamaan kysymykseen, millainen on laadukas tietoturvakulttuuri. Tutkielman aikana on lähestytty laadukkaan tietoturvan aihetta läpikäymällä siihen liittyviä, energiayhtiöitä sitovia lakikokonaisuuksia sekä pyritty löytämään alan ns. best practices -käytäntöjä. Nämä ovat parhaaksi todettuja käytäntöjä tai tekniikoita, jotka yleisesti hyväksytään parhaiksi toimintatavoiksi lakeja tai eettisiä vaatimuksia noudattaen. Lisäksi aihetta on lähestytty läpikäymällä tietoturvan osa-alueet, niiden merkitys yritykselle ja yhteiskunnalle sekä tuotu esille riskienhallintaa ja tietoturvan mittareita. Edellä mainittujen asioiden kautta on pyritty kuvaamaan laadukkaan tietoturvan merkitystä energiayhtiölle.

Lisäksi työssä tutkittiin tietoturvaperehdytysten jalkauttamista ja sen menetelmiä. Perehdyttämistä ja sen ylläpitoa varten oli löydettävä menetelmiä ja suunnitelma niiden jatkuvalle kehittämiselle. Työn tarkoitus oli tunnistaa kohdeyrityksen henkilöstölle soveltuva perehdytysmekanismi soveltaen ymmärrystä ihmisten tavasta oppia. Ihmisen oppimismekanismit, motivaatio, saatu palaute ja halua oppia vaikuttavat suuresti perehdytysten onnistumiseen. Oleelliseksi osaksi oppimista on noussut kerralla annettavan tiedon määrä ja mikro-oppiminen. Näiden lähestymistapojen kautta työssä lähestyttiin kohdeyrityksen henkilökuntaa ensin erilaisilla tietoturvaan liittyvillä kyselyillä ja pilotoinneilla. Näin tunnistettiin perehdytyksiä vaativat asiakokonaisuudet sekä valittiin kohdeyritykselle soveltuvin perehdytysmekanismi. Perehdytysten suunnitteluun otettiin mukaan myös tietoturvan vuosikello.

Viimeisenä aiheena tutkittiin tietoturvan merkitystä työtehtävien perehdyttämisessä. Tutkimuksen eri vaiheissa perusteltiin siinä esiintyvien asioiden tarvetta loppukäyttäjille ja havaittiin, että perehdytysaineiston tulee näin ollen olla riittävän yleisellä tasolla, jotta syntyy ymmärrys, miten se vaikuttaa kunkin työhön ja siinä toimimiseen.

Jatkotutkimusaiheiksi tunnistettiin pelillistämisen luomat mahdollisuudet perehdytyksen jalkauttamisessa sekä tietoturvallisuuskatsausten tuominen mukaan jatkuvaan perehdytysohjelmaan.

Avainsanat: tietoturva, perehdytys, tietoturvakulttuuri, kehitys, mikro-oppiminen, vuosikello

ABSTRACT

Marika Ristolainen: Implementing Information Security in an Energy Company

Tampere University

Degree Program of Management and Information Technology

Examiners: Prof. Marko Seppänen and University Lecturer Rainer Breite

Master's Thesis

April 2020

Information security issues have become one of the biggest concerns of energy companies during last decades. Phishing and scam messages are constantly being received, especially targeting Office365 products. In February 2020, more than 1,300 scam calls were handled in Finland alone. Actual amount of scam calls was probably much higher. These factors alone support the development of information security culture and also careful and constant ongoing initiation in the fight against security crime. Information security culture must be proactive both technology aspect and user awareness aspect. That is worth of investing subject.

The main subject of the study was the development of an energy company's information security culture. The topic of the subject was focused on the development of the implementation and on the selection of a suitable method in the beginning. One aim of the work was to study what quality means in information security culture. During this work, this topic was approached by reviewing laws that are binding on energy companies. So-called Best Practices methods were also searched. These are generally accepted as the best ways to comply with laws or ethical requirements. To improve understanding of information security this work includes areas of information security and their significance for the company and society. By reviewing of risk management and metrics, these subjects were taken among the work. Through mentioned subjects above study tends to describe how important quality information security is for energy company.

In addition, the work examined implementing awareness of security and to develop deployment means. It was necessary to find methods for the maintenance of information security culture and development. The purpose of the study was to find the right orientation mechanism as well as to understand the way people learn. The topic was approached by searching for information on human learning mechanisms. The best mechanisms seem to be motivation, feedback and a desire to learn. Knowledge needs to delivered in small portions. At first, the employees were approached with various fundamental surveys and by piloting. With these steps, the questions were selected for the purpose of the most suitable orientation mechanism. The annual security clock was included for further planning of information security implementation.

Finally, it was estimated how people will understand the importance of information security. This document justifies the need for issues. It was found that the orientation materials must be at sufficiently general level to give an understanding of how it affects each employees work.

The opportunities offered by gaming in the initiation and including information security reviews in the ongoing induction program were identified as the topics for further research

Keywords: information security, orientation, information security culture, development, micro-learning, year clock

ALKUSANAT

Tämä diplomityö on tehty Pori Energia Oy -konsernille kesän 2019 ja alkuvuoden 2020 aikana. Työn ohjaajana ja tarkastajana on toiminut professori Marko Seppänen ja toisena tarkastajana yliopistonlehtori Rainer Breite. Erityiskiitokseni työn ohjaamisesta haluan antaa Markolle, joka on tehnyt suuren työn lukiessaan ja tarkastaessaan työtä sekä antaessaan erittäin arvokkaita sekä laadukkaita kommentteja ja ohjeita työn valmistumiseksi. Erityisesti Markon pehmeä lähestymistapa, mutta kuitenkin suora puhe ovat tehneet kirjoittamisesta helpompaa työn loppuvaiheessa.

Pori Energia Oy:n puolesta työtä on ohjannut ICT-palvelupäällikkö Janne Jansson. Kiitän Jannea erityisesti siitä, että hän on antanut työn suorittamiseen hyviä kehitysehdotuksia kuin myös tuonut mahdollisuuden itsenäiseen työskentelyyn ja oppimiseen. Keskinäisillä lyhyillä sparraushetkillä työ on löytänyt oikean suunnan. Samalla haluan kiittää kollegoja yhteistyöstä uusien O365-mekanismien yhteisistä läpikäynneistä.

Työn tekemisen aikana kohdeyrityksessä oli meneillään useita tietojärjestelmäprojekteja, jotka ajankäytöllisesti vaikuttivat tämän työn tekemiseen sekä koko organisaatioon. Tästä huolimatta työhön on saatu tukea suurelta osalta käyttäjiä sekä sovellusten pääkäyttäjiltä, jotka omalta osaltaan edesauttoivat työn valmistumisessa.

Kumarrus työn valmistumisen mahdollistamisesta kuuluu myös koko perheelleni. Lapsilleni Antille ja Mikolle, puolisolleni Veli-Matille sekä erityisesti omille vanhemmilleni valtavasta tsempistä ja uskosta työn ja koko opiskelun valmistumiseen.

Porissa, 17.4.2020

Marika Ristolainen

SISÄLLYSLUETTELO

LIITE A

Otteita energiayhtiöitä koskevien lakien ja asetusten sisällöstä

KUVALUETTELO

LYHENTEET JA MERKINNÄT

KV11	Kaupunkiverkkoyhtiö, sisältää 11 kaupunkiyhtiötä
2NS	Second Nature Security

1. JOHDANTO

1.1 Tietoturvan yleiskuva

Tietoturva ja sen johtaminen kuuluvat osana kohdeyrityksen toimintaperiaatteita ja ovat tietoturvallisen johtamisen perusta. Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuutta, sen eheyttä ja saatavuuden hallintaa. Tietoturvapolitiikka toimii kaiken tietoturvallisuuden tahtotilana. Sen mukaan yritys on sitoutunut tietoturvallisten työskentelyolosuhteiden ja toimintamallien luomiseen, tietoturvariskien hallintaan, lakisääteisten ja muiden vaatimusten noudattamiseen sekä työntekijöiden osallistamiseen tietoturvan hallinnassa. (Pori Energia Oy Johtoryhmä, 2019)

Tietoturvan tulee koskea koko organisaatiota ja sen tulee sisältyä yrityksen johdon toimenkuvaan ja tehtäviin. Asetettujen tietoturvavaatimuksien ymmärrys on johdon vastuulla ja heidän tavoitteisiinsa tulee sisällyttää toimet, joilla yksilöt voivat ymmärtää asetetut vaatimukset. Johdon tehtäviin kuuluu seurata vaatimusten toteutumista. Johdon vastuulla on myös mahdollistaa tietoturvaohjeistusten tekeminen ja -koulutusten järjestäminen. Ohjeistusten selkeäksi puuttuvaksi osuudeksi on noussut perehdytys sekä jatkuvan tietoturvaosaamisen parantaminen.(Laaksonen, Nevasalo and Tomula, 2006). Tämän työn kautta on tarkoitus perehtyä näihin osa-alueisiin.

Kohdeyritys on tehnyt jatkuvaa tietoturvaohjeistusten uusimista nykyhetken vaatimuksia vastaaviksi. Tietoturvapolitiikka on uudistettu, tietoturvakäytäntöjen ohjeistusta on päivitetty, työasemien oikeustasoja on yhtenäistetty sekä kiristetty aiemmasta (Jansson, 2019a). Näin yritys pyrkii osoittamaan myös asiakkailleen, miten sen organisaatio näkee tietoturvan ja millaisella vakavuudella yritys tietoturvaan suhtautuu.

Työssä perehdytään tietoturvan pehmeiden arvojen korostamiseen yrityksen toiminnassa sekä tietoturvan uudistettujen toimintatapojen jalkauttamiseen ja myöhemmässä vaiheessa jalkauttamisen onnistumisen mittaukseen. Työn aikana suoritetaan monitasoinen uusittu tai täysin uusi ohjeistus eri käyttäjäryhmille riippuen heidän vastuutasoistaan yrityksen toiminnoissa. Samalla täydennetään uuden henkilön perehdytyssuunnitelma, sekin monitahoisena, jolloin mahdollistetaan ihmisten oppimisen erilaisuus. Vielä 2000-luvun alussa Ihmisen vahvimpia oppimisen kanavina pidettiin mm. visuaalista, auditiivista ja kinesteettistä oppimista (Kankaanpään Yhteislyseo, 2019). Jälkeenpäin tehdyissä tutkimuksissa on kuitenkin havaittu, että oppimiseen vaikuttavat voimakkaasti motivaatio oppia, henkilön persoona, ja emootio (Tuomola, Maijanen and Prashnig, 1999a). Pehmeiden arvojen läpivienti oppimistapoineen vaativat tietoturvastrategian tiedostamisen sekä yrityksen johdon vahvan sitoutumisen koko prosessiin. Työn jalkautus vaatii myös asenne- ja kulttuurimuutoksen läpiviennin koko organisaatioon, johon työn aikana etsitään soveltuvat keinot.

Kohdeyritystä säätelevät erilaiset energia-alan säädökset, direktiivit, standardit ja lait kuten sähkömarkkinalaki, päästökauppalaki ja valmiuslaki, joka viittaa tietoturvalliseen

energiantuoton turvaamiseen.(Työ- ja elinkeinoministeriö, 2014) Uusimpana direktiivinä toimii koko Euroopan laajuinen kyberturvallisuuteen liittyvä NIS-direktiivi (European parliament and Council, 2016), joka käsittelee energia-alan kyberturvaa ja astui voimaan 1.6.2019 (European parliament and Council, 2016). Tämän direktiivin tarkoituksena on säätää oikeudellisista toimenpiteistä kyberturvallisuuden yleisen tason parantamiseksi EU:ssa. Edellä mainitut seikat vaikuttavat omalta osaltaan perehdytysaineiston sisältöön, perusasioiden lisäksi.

1.2 Työn tavoitteet ja rajaukset

Työn tavoite on kehittää kohdeyritykselle tietoturvakulttuuri, tarkemmin rajattuna tietoturvaperehdytyksen kehittäminen. Tästä johdettiin työlle kolme tutkimuskysymystä, joihin vastaamalla päästään tavoitteeseen:

1. Millainen on laadukas tietoturvakulttuuri?
2. Miten jalkautetaan, ylläpidetään ja kehitetään tietoturvakulttuuria?
3. Miksi tietoturvakulttuurin on oltava osa työhön perehdytystä?

Työssä paneudutaan tietoturvan pehmeälle puolelle ja tietoturvan jalkautuksen ja perehdyttämisen kokonaisuuden kehittämiseen lähtien perehdytysmateriaalin sisällöstä päätyen materiaalin jalkauttamisen menetelmiin.

1.2.1 Laadukkaan tietoturvakulttuurin ominaisuuksia

Kirjallisuudessa on paljon teoriaa siitä, mitä tietoturvallisuuden tulee sisältää. Tietoturvallisuus on hyvin laaja alue, joten tässä kappaleessa kerrotaan siihen liittyvistä muutamista sen sisältävistä alueista, jotta lukijalle syntyy ymmärrys, millainen on hyvä tietoturvakulttuuri. Klassisessa tietoturvassa on keskitytty teknisiin tietoturva-asioihin kuten virustorjunta, palomuurit sekä muut laitteet ja ohjelmistot. Kuitenkin tietoturvallinen ohjelmistokehitys sekä ihmisten käyttäytyminen ovat nykyaikaisen tietoturvan erityisiä mielenkiinnon kohteita, joista tässä työssä tullaan perehtymään tarkemmin jälkimmäiseen. Oleellista on ymmärtää, että niin tekniikka, käytetyt ohjelmistot ja sovellukset ja niiden tietoturva on tärkeää, mutta tärkeimmän osan tietoturvallisuudesta muodostavat ihmiset, jotka käyttävät näitä tekniikoita. Käytetyn tekniikan perusymmärrys auttaa käyttäjiä käsittämään, mitä asioita se ei hoida ja mikä jää yksilön vastuulle. Kaikkia asian kanssa toimivia tulee tukea sekä asioista tulee puhua ja tiedottaa avoimesti. Tietoturvakulttuuri muodostuu kaikista näistä osa-alueista sekä niiden keskinäisestä toiminnasta ja toiminnan hyvyydestä. Tietoturvakulttuurin kehittäminen on yksi osa tätä kokonaisuutta. Työssä otetaan kuitenkin kantaa nimenomaan kohtaan 6. Peruskäyttäjien tukeminen perehdytysohjelman kautta (ks. Kuva 1).

Kuva 1: Tietoturvallisuuden kokonaisuus (Valtionvarainministeriö, 2006)

Tietoturva on siis kaikkien edellä mainittujen ja kuvassa näkyvien asioiden muodostama kokonaisuus, josta tässä työssä käsitellään suurimmaksi osin sen kehittämistä (kohta 1 ylläolevassa kuvassa) sekä sen viestinnän menetelmiä (kohta 3) sekä peruskäyttäjien tukemista (kohta 6).

Aiemmin tietoturvan jalkauttaminen on käytännössä ollut erilaisten ohjeiden luomista ja niiden säilömistä jonnekin yrityksen tallennuspaikoista. Opetus on pidetty esitelmänomaisesti tai luennoin. Näin on voitu korostaa niitä asioita, mitä kouluttaja on itse nähnyt oleellisiksi. Tietoturvan jalkauttamisessa kuitenkin paras anti saadaan, kun tietoa jaetaan pienien asiakokonaisuuksien kautta ja näin mahdollistetaan asian sisäistäminen. Tavoitteena voidaan pitää mikro-oppimisen mallia, jossa tietoa annetaan pienissä erissä, mutta jatkuvasti (Leino, 2019a). Jalkauttamisen tulee myös olla jatkuvaa. Työssä käyttöön otettava tietoturvan vuosikello tuo ratkaisumallin jatkuvuuden suunnitteluun ja toteutukseen. Vuosikello mahdollistaa myös tietoturvan kehityssuunnitelmien teon tuleville vuosille (Plandisc, 2020), jolloin suunnittelun vaiheet ja kehitystavoitteet ovat läpinäkyviä kaikille asiaa tarkasteleville.

1.2.2 Tietoturvakulttuuri osana työhön perehdytystä

Energiayhtiössä työskenteleviä ihmisiä säätelevät erilaiset lait, joiden kautta heille tulee myös tiettyjä velvoitteita. Riippuen henkilöiden työtehtävästä, voi perehdyttämisen sisältö ja syvyys olla erilaista. Tietoturvan ymmärrys ja sen määrittämien toimien ymmärtäminen on kuitenkin jokaisen työntekijän tehtävä ja edellytys, jotta yritys voi toimia alalla turvallisesti. Perehdytys antaa myös tietyn yrityskuvan, varsinkin uusille työntekijöille ja vaikuttaa näin yrityksen imagoon. Tietoturvan perehdytyksen minimointi varsinaisen perehdytysohjelman aikana saattaa aiheuttaa vaaran, ettei työntekijä tiedä, mitä tietoturvallisuusriskejä tulee varoa ja miten toimia. Tämä puolestaan saattaa aiheuttaa haittaa yritykselle, rikkoa tiedon eheyttä, saatavuutta ja luottamuksellisuutta. Mikäli perehdytystä ei ole järjestetty asianmukaisesti, voi työntekijä vedota

virhetilanteessa, ettei ole saanut tarpeeksi tietoa asian välttämiseen. Vastuu työhön perehtymisessä on kuitenkin molemminpuolinen – niin perehdyttäjällä läpikäydä asiat ja perehtyjällä kysyä asioista.

Seuraavassa kerrotaan niistä asioista, jotka tietoturvaan yleisesti vaikuttavat. Näiden kautta kootaan tietoturva-asioiden kehyskokonaisuus.

2. TIETOTURVA, RISKIENHALLINTA JA PEREHDYTYKSEN JALKAUTTAMINEN

Tietoturvallisuuden kokonaisuus koostuu erilaisista osista. Näistä teknisiä osia edustaa toimintaympäristö, jonka varassa yrityksen toiminta on eli tietoverkot, palvelimet, kytkimet ja muu tekninen välineistö. Ohjelmistoturvallisuus sisältää käyttäjätietoihin kuuluvia asioita, kuten pääsyoikeudet ja niiden todentaminen. Ohjelmistojen käytön tulee olla tietoturvallista. Osana yrityksen tietoturvaa ovat päätelaitteiden turvaaminen sekä kulunvalvonnan turvaaminen ja valvonta. Lisäksi yritysten tulee noudattaa niitä lakeja ja asetuksia, jotka sen toimintaa säätelevät. Henkilöstön turvallinen toiminta sitoo näitä osa-alueita toisiinsa.

Yrityksen tietoverkolla tarkoitetaan mm. palvelinratkaisuja, käyttöjärjestelmiä, tietoverkkoja ja tietoturvaa. NIST eli National Institute of Standards and Technology käsittelee eri alojen suosituksia ja standardeja ja ottaa kantaa mm. infran kyberturvauhkiin ja tuottaa infran Best Practices -suosituksia. NIST toimii pääasiassa Yhdysvaltojen hyväksi pyrkien tukemaan maan innovoimaisuutta ja teollisuuden kilpailukykyä. NIST tuottaa kyberturvallisuusohjelmia, joiden kautta pyritään mahdollistamaan aiempaa paremmat käytännöt tietotekniikan ja sen menetelmien kehittämiseen ja käytäntöön soveltamiseen.(NIST, 2019). Infran tietoturvan vaiheiden läpikäyntiä ei tässä työssä käsitellä laajemmin.

Työntekijän käytettävissä olevan ohjelmiston käyttäjätietojen hallinta, käyttäjien todennus sekä pääsyoikeudet ovat tekijöitä, joilla voidaan turvata tietoturvallinen käyttö. Näissä voidaan ottaa kantaa myös mahdolliseen tietojen turvaluokitukseen. Ohjelmiston tietoturvallinen käyttö on osa perehdytystä ja sitä kautta osa tietoturvakulttuuria. Ohjelmistojen koulutusta järjestetään usein pääkäyttäjien toimesta, mutta uuden henkilön ollessa kysymyksessä, myös kollegoiden kautta, joten tietoturvan ymmärrys koko yrityksessä on erittäin tärkeää.

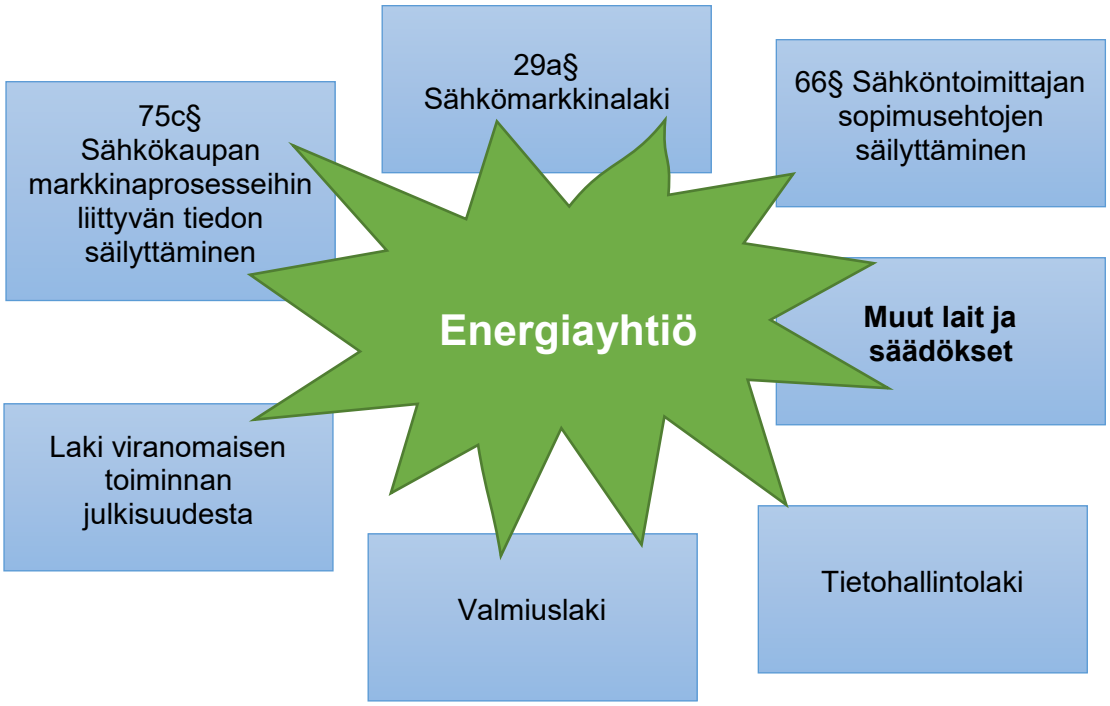
Valtiohallinnon tietoturvallisuuden johtoryhmän henkilöitä, päätelaitteita ja kulunseurantaa koskevat määrittelyt soveltuvat erittäin hyvin kohdeyrityksen käyttöön. Kohdeyritys toimii yhteiskunnalle merkittävässä roolissa taatessaan yhteisön eri toiminnoille sekä sähköä että lämpöä. Näin ollen energiayritykset noudattavat Suomen kyberturvallisuusstrategiaa ja ovat velvoitettuja kriisitilanteissa toimimaan yhteiskuntaa sitä tukevissa tehtävissä.

Päätelaite, eli työasema, voi olla suojattu esimerkiksi tietoturvasirulla. Vaihtoehtoisesti päätelaite voi olla tavallaan ”tyhmä” pääte, jota käytetään ns. virtuaalityöpöydän käynnistämiseen. Nämä virtualisoinnin kautta toimivat työpöydät vaativat omat tunnistusmekanisminsa ja näin päätelaitteen kautta ei päästä yrityksen tietoihin käsiksi. (Kansainvälinen Kauppakamari, 2019). Kohdeyritys on hyödyntänyt näitä mekanismeja. Käyttäjätunnistuksessa voidaan hyödyntää perinteistä käyttäjätunnus – salasana -mekanismia monimutkaisempia tapoja, kuten kasvotunnistusta, sormenjälkitunnistusta ja jopa silmän iiriksen tunnistusta. Oikea, tunnistettu, käyttäjä pääsee haluamaansa sovellukseen opeasti ja turvallisesti. (Microsoft, 2020).

Toimitilaturvallisuus on yksi osa-alue turvallisuuden hallinnassa. Se sisältää mm. kulunvalvonnan, teknisen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä erilaisten lähetysten (kuten posti, kuriiri tmv.) turvallisuuden (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013). Kohdeyrityksessä toimitilaturvallisuuteen kiinnitetään entistä enemmän huomiota vieraiden liikkumiseen toimitiloissa ja näihin liittyviin ohjeistuksiin. Edellä mainitut osa-alueet muodostavat suuren osan yrityksen tietoturvakulttuurista.

2.1 Energiayhtiöiden toimintaa säätelevät lait

Energiayhtiöissä käsitellään sekä julkista (esim. käyttöpaikkatiedot), että salaista (esim. asiakastiedot) tietoa. Julkisuuslaissa (Oikeusministeriö, 1999) on määritelty, että tieto on julkista, ellei sitä ole erikseen laissa määritelty salaiseksi. Suomen laista löytyy useita erilaisia tietoturvavelvoitteita. Tietoturvan toteuttaminen on siis säädetty laissa ja näin ollen se tulee hoitaa asianmukaisesti. Kaikki lait koskevat kohdeyritystä, mutta osa niistä säätelee erityisesti energiayhtiöiden tietoturvalle asetettuja vaatimuksia. Näitä ovat mm. Perustuslaissa mainittu sähkömarkkinalaki 29a§, sähköntoimittajan sopimusehtojen säilyttäminen 66§, sähkökaupan markkinaprosesseihin liittyvän tiedon säilyttäminen 75c§ sekä salassapitovelvollisuus ja hyväksikäyttökielto 76§. Näiden lisäksi energiatoimialaa säätelevät seuraavat lait: laki viranomaisen toiminnan julkisuudesta, valmiuslaki sekä tietohallintolaki. Kuva 2 esittää kokonaisuutta laista, jotka säätelevät ja ohjaavat energiayhtiöitä Suomessa.



Kuva 2: Energiayhtiöiden tietoturvaa käsitteleviä lakeja

Näiden lakien noudattaminen on ensiarvoisen tärkeää tiedon eheyden, luotettavuuden ja saatavuudenhallinnan takaamiseksi kaikissa olosuhteissa. Kohdeyrityksen toimintaa säätelevien lakien sisältö on läpikäyty tarkemmin tutkielman lopusta löytyvässä dokumentissa (LIITE A

Otteita energiayhtiöitä koskevien lakien ja **asetusten sisällöstä**).

2.2 Tietoturvallisuuden merkitys yritykselle

Tietoturvallisuuden käsite on monelle työntekijälle vaikea ymmärtää. Tässä työssä läpikäydään tietoturvallisuuden tärkeyttä siitä syystä, että työntekijät näkisivät sen merkityksen heille itselleen, kodilleen, yhteiskunnalle ja työnantajalle. Nämä muodostavat jokaisen työntekijän elinympäristön, jonka suojaaminen on meidän kaikkien tehtävä. Samalla on toivottavaa nähdä oma roolinsa työntekijänä yrityksessä ja merkityksensä yhtenä osana tietoturvan kehittymistä yhteisössä.

Nykypäivän yhteiskunta painottuu ja nojautuu suurilta osin tietoteknisiin toimintoihin. Teemme jatkuvaa tietoteknistä yhteistyötä eri yhtiöiden, viranomaisten ja sidosryhmien kanssa, jolloin tietoturvallisuus yltää jokaisen eri organisaation yksilöön ja jokaisella on vastuu sen toteuttamisesta. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013). Koska suurimmat tietoturvaan liittyvät ongelmat lähtevät henkilöistä ja heidän kiireestään, huolimattomuudestaan sekä osaamattomuudesta sen lisäksi, että siihen liittyvät tietojärjestelmien toteutuksen ja käytön laadukkuus, on erittäin tärkeää, että tietoturvaan liittyvät toimet ja ohjaus huolehditaan kaikissa portaissa. Yhden heikkous on koko ketjun heikkous. Tietoturvallisuuteen kohdistuvat väärät asenteet, toimintatavat sekä puutteellinen ohjeistus vaikuttavat asiakkaiden ja yhtiön edut sekä teettää lisätyötä sekä lisäkustannuksia. (ICT Standard Forum, 2019c) Tietoturvan laiminlyönnin seurauksena yrityksen kärsii mainehaitoista sekä taloudellisia tappioita. Tätä kautta tietosuojaloukkaus vaikuttaa yrityksen taloudellisiin lukuihin. GDPR-säädöksen seurauksena voi aiheutua tuntuvia sakkorangaistuksia, mikäli tietoturvaloukkaus on syntynyt. Kuitenkin tietosuoja on vain osa tietoturvaa.

Tietoturvariskin syntyminen ja aikaansaaminen on helppoa. Työasema tai mobiililaite jää junaan, lentokentälle, taksiin tai käyttäjä klikkaa auki tietojenkalasteluviestin sähköpostistaan. Mikäli työasemaa tai mobiililaitetta ei ole suojattu asianmukaisesti esimerkiksi näytön lukituskoodilla, sormenjälkitunnistuksella tai edes riittävällä ja monimutkaisella salasanasuojauksella, voi yrityksen ulkopuolinen henkilö päästä käsiksi yrityksen tietoihin ja tehdä haittaa yritykselle. Työntekijöiden säännöllinen perehdytys ja kouluttaminen sekä avoin tiedotus erilaisista uhkatekijöistä auttaa tietoturvauhkien ymmärryksessä. Henkilöstö onkin, monen tutkimuksen mukaan, yksi yrityksen merkittävimmistä tietoturvariskeistä, joten on tärkeää, että jokainen työntekijä ymmärtää tietoturvan toimintaohjeiden tärkeyden. Näiden lisäksi teknistä tietoturvaa tulee kehittää jatkuvasti ja ennakoiden tietoturvaloukkauksia. (Jokinen, 2019)

2.2.1 Tietoturvan käsite

Mitä tietoturvalla sitten tarkoitetaan? Tietoturva on tärkeää, joten sen sisältöä kannattaa hieman tutkiskella. Seuraavassa avataan tietoturvan käsitettä suomalaisen yhteiskunnan mittakaavassa, jotta syntyy ymmärrys aluelaajuudesta, joita tietoturvallisuus käsittelee.

Tietoturvatoimenpiteet ovat yksilön, yhteisön ja yhteiskunnan etujen suojausta varten. Tietoturvajärjestelyjen tarkoitus on varmistaa, että tietoaineistot, -järjestelmät ja palvelut on suojattu asianmukaisesti ja että niiden luottamuksellisuus, eheys ja saatavuus ovat

mahdollisimman riskittömiä (C.I.A = Confidence, Integrity, Availability). Tällä tarkoitetaan, että tiedot ja tietojärjestelmät ovat vain niille tarkoitettujen henkilöiden ja tahojen käytettävissä, heille osoitetuissa työtehtävissä, eivätkä ne saa tulla julki, muuttua tai tuhoutua hallitsemattomasti. Tietojen tulee myös olla saatavilla aina, kun niitä tarvitaan. Verkottuneessa yhteiskunnassa tietoturva on toimintojen, palveluiden, sovellusten ja tietotekniikan infran perusedellytys. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013). Tietoturva on tietoaineistojen suojaamista ts. sillä tarkoitetaan yhtiön omistamien tietojen, tietojärjestelmien sekä palveluiden asianmukaista turvaa siten, että niiden luottamuksellisuus, eheys ja käytettävyys ovat hallittuja. Tähän liittyy vahvasti käyttöoikeuksien asianmukainen luovutus oikeille tahoille, oikeaan tehtävään sekä näiden tietojen salassapito. Tietoturvan kautta ylläpidetään tietojen, järjestelmien ja palveluiden toimintaa ajallaan. Näiden toimintojen kautta turvataan niin yksilön, yhteisön kuin yhteiskunnankin etuja. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013).

Vuonna 2018 voimaan tullut Tietosuojalaki säätää järjestelmien käytöstä jäävästä tapahtumalokista, jotta tarvittaessa voidaan jälkikäteen selvittää erilaisia järjestelmän käyttöön liittyneitä tapahtumia (Oikeusministeriö, 2019). Tästä on myös tehty erillinen Valtiohallinnon VAHTI -ohje, jossa käsitellään tarpeelliset ICT-lokitukset, niiden käsittely ja vastuut sekä prosessit, järjestelmähankintoihin kohdistuvat lokinäkökohdat sekä niiden säilytys, kerääminen ja suojaaminen (Valtiovarainministeriö, 2009a). VAHTI-ohjeistukset ovat kohdeyritykselle merkityksellisiä ohjeistuksia niiden ohjatessa perusturvaa ylläpitäviä laitoksia.

Tietoturva on koko yhteiskunnan perusedellytys ja se tekee siitä jokaisen organisaation työntekijän velvollisuuden. Nykyajan jatkuva kiire ja huolimaton toiminta aiheuttavat suurimman osan tietoturvaan liittyvistä ongelmista, jolloin vaarannetaan yrityksen ja sen asiakkaiden sekä työntekijöiden etuja. Näiden asioiden ehkäisy sekä korjaavat toimenpiteet aiheuttavat lisätöitä ja sitä kautta kustannuksia. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013) Tietoturvan tarkastelu voidaan tehdä eri alueille, riippuen siitä, miten luokitteluja halutaan tehdä. Oleellisena osana työtä puhutaan tietoturvan jalkauttamisesta, jolloin oletusluontoisesti perusinfra on kunnossa ja yrityksen sisäinen verkko suojattu. Käytössä olevien päätelaitteiden eli tietokoneiden, tablettien, puhelimien ja muiden vastaavien laitteiden tulee sisältää mahdollisimman vähän luottamuksellista tietoa. Päätelaitteet tulisi suojata tunkeutumisenesto- järjestelmällä, joka salaa niissä olevan tallennetun tiedon. Tietoverkkoja tulee kontrolloida jatkuvasti, jotta poikkeamia tai tietomurtoja ei pääsisi tapahtumaan. Myös palautustoimien tulee olla riittävän tehokkaita. Yrityksen tietoja sisältäviä tietovarastoja tulee suojata tiedon kriittisyysasteen mukaisin keinoin. Hyviä luokitteluja ovat sisäinen, salainen tai julkinen. (ICT Standard Forum, 2019b)

Tietoturva ei ole vain tekniikkaa ja teknisiä laitteita. Osa tietoturvaa on identiteetinhallinta (Identity and Access Management, IAM), jonka suunnittelu tulee tehdä huolellisesti ja ennakoivasti. Mikäli identiteettivarkauksia tapahtuu, voi siitä olla seurauksena ulkopuolisten pääsy yritykselle luottamuksellisiin tietoihin, tietojen kopiointi ja/tai käyttö luvattomasti, data tuhoutuu tai siitä tulee epäkuranttia. Tietoturvan heikoin lenkki on usein yrityksen työntekijä. Siksi on oleellista pyrkiä välttämään inhimillisiä virheitä tukemalla ja ohjaamalla käyttäjiä, perehdyttämällä heitä säännöllisesti tietoturva-asioissa, tiedottamalla uhista ja määrittelemällä riittävät, mutta rajaavat käyttöoikeudet liiketoiminnan järjestelmiin. (ICT Standard Forum, 2019b) Tietoturvaan liittyvät toimenpiteet ovat siis kaikki määritelty, jotta yksilön, yhteisön ja yhteiskunnan etujen

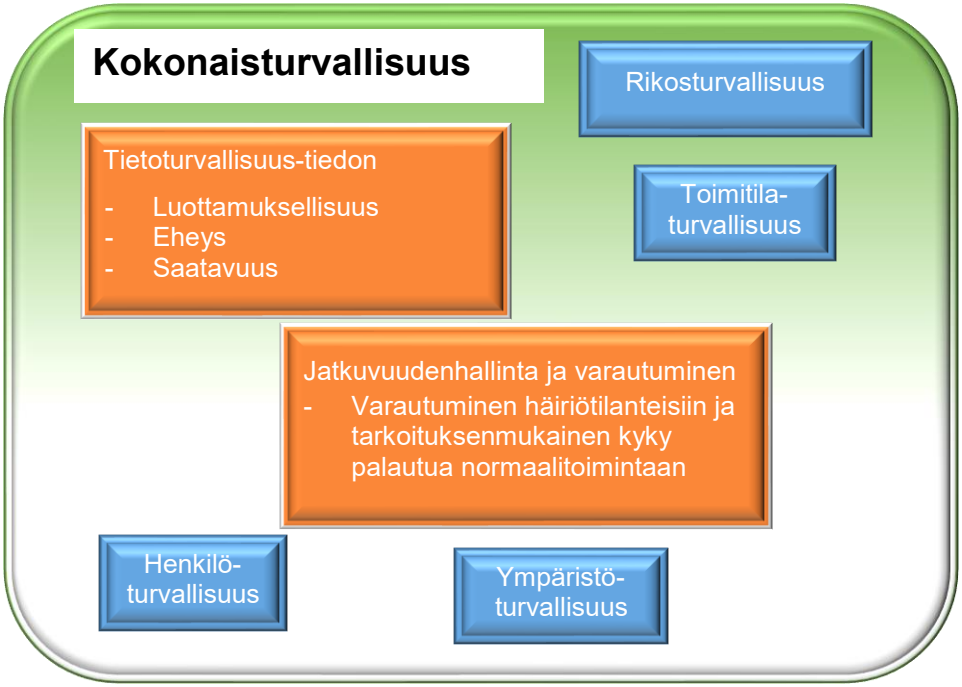
suojaus pystytään hoitamaan. Seuraavassa pureudutaan edellä mainittujen seikkojen hoitamiseen liittyviin tietoturvallisuuden osa-alueisiin hieman tarkemmin.

2.2.2 Tietoturvallisuuden osa-alueet

Tietoturvallisuuden kokonaiskuvan hahmottamiseksi on työhön otettu mukaan sen osa-alueiden käsittely. Tietoturva koskee yllättävän monelta suunnalta jokaista työntekijää ja heidän vastuitaan toimia tietoturvallisesti. Asian hahmottaminen saattaa olla vaikeaa, josta syystä perehdytystavalla on tärkeä rooli oppimisessa. Tietoturvakulttuuri ottaa huomioon jokaisen alueen ja näitä kaikkia pyritään kehittämään kokonaisuuden kehittymiseksi.

Tietoturva jakautuu perinteisesti erilaisiin kokonaisuuksiin ja sitä kautta osa-alueisiin. Tietoturvan kokonaisuuden turvaamisessa tulee siis huomioida kaikki osa-alueet, jotta voidaan varautua erilaisiin uhkiin sekä hallita paremmin kokonaisuutta. Tietoturvakulttuurin sisällä eri alueiden lisäksi puhutaan toiminnoista, joiden avulla osa-alueita ohjataan ja kehitetään. Myös niihin tulee kiinnittää huomiota perehdytyksessä.

Tietoturvallisuuden osa-alueet on läpikäyty seuraavassa päällisin puolin, jotta kokonaiskuva syntyy. Lisäksi on käytetty visuaalista kuvausta asian ytimen avaamiseksi. Kuva 3 esittää kokonaisturvallisuutta.



Kuva 3: Tietoturvallisuus ja jatkuvuuden hallinta ja varautuminen ovat osa suurempaa turvallisuuskokonaisuutta (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013)

Henkilöstöturvallisuuden tulee olla suunnitelmallista ja järjestelmällistä, henkilöstöä kehittävää toimintaa, jota johdetaan niin yrityksen johdon kuin henkilöstöasioiden hallinnon suunnasta. Moni tietoturvarikkomus on organisaation menettelytapaohjeiden aiheuttamaa.(Valtiovarainministeriö, 2009b) Työn aikana kiinnitetään huomiota tietoturvan perehdytykseen ja sen jalkauttamiseen sellaisilla toiminnoilla, joilla jokaisen

kohdeyrityksen työntekijän on helppo ymmärtää tietoturvallisen toiminnan merkitys yritykselle sekä omaan työhön. Samalla perehdytysohjelmaan liitetään suurempana osana tietoturvallisuusasiat uusille työntekijöille sekä vuosisuunnitelma nykyisille työntekijöille.

Henkilöstöturvallisuus sisältää työn johtamisen, sen valvonnan, tiedonkulun ja yhteistyön sekä teknologian, koko yritysorganisaation ja yksittäisen henkilökunnan jäsenen sekä hänen työnsä ja työympäristön välisen yhteyden. Henkilöstöturvallisuus sisältää myös työntekijöiden tietoturvallisuuteen sisältyvät vastuut sekä velvoitteet. (Valtiovarainministeriö, 2009b) Hyvä esimerkki velvoitteista on työsopimukseen sisällytetty salassapitovelvollisuus -pykälä, kuten kohdeyrityksellä on tehty. Sama velvoite on sisällytetty urakoitsijoiden sekä toimittajien sopimuksiin. (Jansson, 2019b). Nämä merkinnät tulee kirjata myös henkilöstörekisteriin. Henkilöstöriskeihin luetaan myös työsuhteen päättymiseen liittyvät riskit, varsinkin riitatilanteissa (Valtiovarainministeriö, 2009b). Kohdeyrityksessä tähän on varauduttu kirjaamalla yhteiset ohjeet käyttäjätunnusten käsittelyä varten. Niin IT-toimittaja kuin kohdeyrityksen tietohallinto-osasto vastaavat ohjeiden toteutumisesta.

Fyysisen turvallisuuden eli toimialaturvallisuuden tarkoitus on suojata yrityksen toiminta kaikissa olosuhteissa. Tähän kuuluvat mm. kulunvalvonta, kameravalvonta, vartiointi ja tekninen valvonta sekä vesi-, palo-, sähkö- ja murtovahinkojen torjunta. Tämä turvallisuusalue on kiinteistöhallinnon tai rakennuksen omistajan vastuulla. Suojaukset tulee toteuttaa turvallisuusluokitusten mukaisesti. (Valtiovarainministeriö, 2009b). Kohdeyrityksessä tästä vastaa laitospalvelupäällikkö (Pori Energia Oy Johtoryhmä, 2019).

Tietoliikenneturvallisuus sisältää tietoliikenneyhteyksien turvatun yhteydenpidon etätyöpisteisiin, etähallintaan, älypuhelimien yhteyksien sekä niiden käytön turvallisuuden, lähiverkkoon liittyvät suojaukset, poikkeusoloihin varautumisen ja kaikkiin edellä mainittuihin liittyvät tekniset ratkaisut. (Valtiovarainministeriö, 2009b)

Laitteistoturvallisuuteen luetaan kuuluvaksi esim. kytkimet, digiboxit, puhelimet, työasemat sekä erilaiset päätelaitteet, tietovarastot ja tietoverkot. Työvälineiden sekä verkossa toimivien laitteistojen tulee olla yrityksen hallinnassa sekä valvonnassa. (Valtiovarainministeriö, 2009b). Ilman asianmukaisia toimenpiteitä eivät internet, yrityksen tietoverkko tai laitteistot ole turvallisia. (Kansainvälinen Kauppakamari, 2019) Myös laitteistojen käyttöikää tulee valvoa, jotta niiden ajanmukaisuus ja turvallisuus on taattu. Jokainen laite, joka liitetään verkkoon, tulee tunnistaa. Esimerkiksi työasemat, joissa on vanhentuneita käyttöjärjestelmiä (esim. Windows 7 tai vanhempi) ei saa liittää verkkoon hallitsemattomasti (Jansson, 2019b).

Ohjelmistoturvallisuudella tarkoitetaan yrityksen omien sovellushankintojen tietoturvallisuuden huomiointia sekä sosiaalisen median tuomia sovelluksia. Ohjelmistoturvallisuus tarkoittaa myös käyttöjärjestelmien sekä virustorjuntojen ja palomuurien ajanmukaisuutta tietoturvallisuuden takaamiseksi. Näiden toimien kautta luodaan turvallisuutta työntekoon. Työntekijöiden oma toiminta on kuitenkin oleellinen osa ohjelmistoturvallisuutta. Uhkia muodostavat erilaiset ryhmittymät sekä valtiot, joiden tarkoituksena on saada haltuunsa erilaisia tietoja, kuten luottokortti- ja henkilötietoja ja pyrkimykset vaikuttaa esimerkiksi päätöksentekoon. (Valtiovarainministeriö, 2009b)

Tietoaineistoturvallisuus liittyy sähköisten palveluiden tietoturvallisuuden keskeisiin kohtiin. Näitä ovat mm. sähköinen asiointipalvelu, asiakaspalvelujärjestelmä, taustajärjestelmä palvelun tarjonnalle sekä muut sähköiset järjestelmät kuten sähköposti, VPN-yhteydet, DA-yhteydet. (Valtiovarainministeriö, 2009b)

Käyttöturvallisuudella tarkoitetaan käyttäjän tunnistamista eri verkkopalveluissa sekä sen eri tasoja huomioiden tunnistuksen vahvuus.(Valtiovarainministeriö, 2009b). Hallinnollinen ja organisatorinen tietoturvallisuus tarkoittaa yrityksen tietojen sekä palveluiden, että tietoliikenteen sekä järjestelmien suojaamista ja varmistamista siten, että niihin kohdistuvat riskit hallitaan sekä poikkeus- että normaalioloissa. (Valtiovarainministeriö, 2009b).

Edellä mainittujen lisäksi kokonaisturvallisuuteen liittyvät ympäristöturvallisuus, toimitilaturvallisuus sekä rikosturvallisuus, jotka on kuvattu aiemmin, Kuva 1. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013).

Uusien teknologioiden yleistyessä, on tietoturvakulttuurin kehitys ulotettava myös pilvipalveluihin. Myös kohdeyrityksessä on otettu käyttöön uusia O365-välineitä, joten yrityksen henkilöstön perehdyttäminen niiden tietoturva-asioihin on oleellista. Microsoft on siirtänyt lyhyessä ajassa useita palveluitaan ns. pilvipalveluihin. Palveluita ja tuotteita markkinoidaan kokonaisuuksina, joihin yritysten, yhteisöjen ja valtiohallintojen, yhdessä kuluttajien kanssa, on mahdollista hankkia laajennusosia. Kohdeyritys onkin siirtynyt vuonna 2019 käyttämään pilvipalveluita joidenkin tuotteiden osalta. Perusteena O365-välineiden käytölle ovat olleet niiden tietoturvallinen käyttö sekä tuotteiden käytön mukainen laskutusmalli. Käyttöönotettu O365-palvelukokonaisuus sisältää tällä hetkellä muun muassa sähköpostin, kalenterin, OneDrive -pilvitallennustilan sekä viestintä- ja työryhmäsovelluksia, kuten Teams ja Planner. Aiemmin käytössä ollut Skype for Business -viestintäsovellus on jäämässä vähitellen pois käytöstä, myös Microsoftin toimesta.

Tietoturvallisuuden näkökulmasta tarkastellen pilvipalvelut tuovat selkeitä etuja. Ne tarjoavat turvallisen, ajasta ja paikasta riippumattoman työskentelyn kaikille yrityksen työntekijöille. ”Pilvipalveluiden myötä myös kalasteluviestit ja virussähköpostit tulevat määrällisesti pienenemään uusien tehokkaampien estokeinojen avulla”, kertoo ICT-palvelupäällikkö Janne Jansson (Jansson, 2019b). O365 tuo tullessaan myös kaksivaiheisen tunnistuksen, joka suojaa käyttäjätilin sekä sen salasanan. Kaksivaiheisen tunnistuksenkäyttöönotto edellyttää älypuhelimeen Microsoft Authenticator -sovelluksen latausta. Mikäli kyseistä sovellusta ei ole, käyttäjän varmennus tapahtuu tekstiviestin kautta. Näin turvataan, että käyttäjä on tunnistettu yrityksen henkilökunnaksi hänen kirjautuessaan yrityksen verkon ulkopuolelta palveluihin. Tämä mahdollistaa myös kotikoneen käytön esimerkiksi postien luvussa.(Kaukosalmi, 2019) Teams -viestintäsovellusta on kohdeyrityksessä hyödynnetty muun muassa viestintäkanavina eri tiimien kesken sekä koko yritykseen kohdistuvassa viestinnässä, tietoturvauhista kertomisessa, ohjeistuksessa ja muussa vastaavassa toiminnassa. Näin Teams samalla toimii Wisdom of Crowds -tyyppisen toiminnan pohjana ja tukena. Tiimit jakavat kanavillaan tietoja ja neuvoja ja näin voidaan sanoa, että ”sana leviää”. Teams on erittäin nopea tiedonvaihtoväline ja tietohallinto onkin käyttänyt sitä nopeaan tiedotukseen ja ohjeistukseen sähköpostin ja kirjallisen muun viestinnän ohella. Planner puolestaan toimii tehtäväkortistona sekä myös tietohallinnon strategian suunnittelussa apuna. Tietoturvan näkökulmasta

pilvipalveluissakin on olemassa aukkoja. Näiden esiintymistä ja kehitystoimia seurataan kohdeyrityksessä jatkuvasti sekä suoritetaan tarvittavia korjaustoimenpiteitä yrityksen turvallisen toiminnan takaamiseksi.

2.2.3 Tietohallinnon mittarit

Kohdeyrityksen tietohallinnolle ei ole aiemmin määritelty selkeitä tavoitemittareita. Tavoiteasetannan yhteydessä on sovittava tietohallinnon mittareista, joilla tavoitteiden saavuttamista ollaan mittaamassa. Lisäksi sovitaan, mitkä asiat riittävät mittarin täyttymiseen. Mittareiden tulee kuitenkin olla riittävän hyviä kuvaamaan tavoitteita. Liian suuri määrä mittareita tai väärät mittarit eivät anna oikeaa kuvaa. Näitä onkin seurattava jakson aikana, jotta niiden ohjaavuus tulee saavutettua.

Työn aikana tulee mietittäväksi, soveltuvatko esimerkiksi vuosittaisen tietoturvaohjeistuksen noudattaminen sekä henkilökunnan tietoturvatestit mittauksen kohteiksi osana kokonaismittaristoa. Riskinä mittaristolle voi olla liiallinen laajuus. Mittariston tulee olla vertailukelpoista, jotta tulokset ovat luotettavia. Tähän vaikuttavat tietoturvan osalta eritasoiset käyttäjäryhmät ja heitä koskevien tietoturvaohjeiden erilaisuus. Mittareiden tulee olla myös ennakoivia, jotta tietohallinnolla on mahdollisuus tehdä muutoksia niille asetettujen tavoitteiden saavuttamiseksi. Mittareille tulee asettaa suunnitellulle ajanjaksolle tavoitearvot ja niiden hyväksyntää ohjaavat raja-arvot. Vastaavista energiayhtiöistä on saatavilla vertailuarvoja, joten tuloksia voidaan analysoida niitä vasten varsinkin mittauksen alkuvaiheessa, kun omaa historiatietoa ei vielä ole. Yhtenä mielenkiintoisena mittarina voitaisiin ajatella toimivan kalasteluviesteihin liittyvä koulutus, tiedotus, testiviestintä sekä niiden tuloksena saadut arvot, esim. puolivuosittain. Tietoturvakoulutusten ja tiedotusten tarkoituksena on saada viesteihin liittyvää virhetoimintaa vähentymään ja testiviestien avulla voidaan nähdä, vaikuttavatko tietoturvatoimet ihmisten käyttäytymiseen eli oppimiseen. Tämän aihealueen mietintä tulee lisätä osaksi työn jatkotoimia, kun perehdytysohjelma on käynnistetty. Luotuja mittareista voidaan jatkossa käyttää tietohallinnon tavoitteiden saavuttamiseen sekä sidosryhmäviestintään. Mittarit ovat myös tietohallinnon johtamisen välineitä, mikäli ne kattavat toimintoja riittävän laajasti. Asetettujen mittareiden tulee olla ajantasaisia sekä havainnollisia, jotta niistä on todellista hyötyä tietohallinnolle ja yrityksen johdolle.

Muita tietohallinnolle soveltuvia mittareita ovat mm. sovelluksiin liittyvät mittaukset, kuten kustannusten seuranta uuden sovelluksen käyttöönotossa tai uuden palvelualustan käyttöönotto ja perustietotekniikkakustannukset. Mittarina voidaan pitää myös ajallisia mittauksia, kuten projektin läpimenoaika vs. suunniteltu läpimenoaika. Tietohallinnossa asiakkaaseen kohdistuva palvelukyky on mittaamisen arvoinen asia, samoin asiakastyytyväisyyskyselyt.

On tärkeää muistaa, että tietohallinnon mittarit ovat riippuvaisia organisaation tietohallinnolle asettamista tavoitteista ja niiden tavoittamisesta. (ICT Standard Forum, 2019c). Mittareihin liittyvien tunnuslukujen tarkoituksena on motivoida ja palkita työntekijöitä, sillä mittaus kertoo organisaation onnistumisesta ymmärrettävästi pitkällä aikavälillä. Mittauksen tavoitteita ovat luotettavan ja tarkan informaation tuottaminen ja samalla se kertoo organisaatiolle tärkeistä asioista. Koska mittareiden tehtävä on ohjata organisaatiota, tässä tapauksessa tietoturvaperehdytyksen kehittymistä, oikeaan

suuntaan, kertovat mittarit nopeasti syy-seurausketjun ja mahdollistavat työhön tarvittavat muutokset. (Manninen, Suomala and Lyly-Yrjänäinen, 2018) Mittareiden ja mittaamisen merkitys tietoturvakulttuurin kehittämisessä nousee osaksi jatkokehitystoimia.

2.3 Riskienhallinta tietoturvan osana

Riski-sanalla kuvataan jonkinlaiseen onnettomuuteen tai tapahtumaan mahdollistavaa vaaraa, onnettomuuden todennäköisyyttä ja sen seurausten yhdistelmää. Sanan riski synonyyminä voidaan pitää epäonnistumista. (Ahponen, 1997). Riskien ottaminen tietoturva-asioissa tuottaa suoran yhteyden vaaraan, jota välttääkseen jokaisen työntekijän tulee perehdytyksen kautta saada laaja ymmärrys, mitä tietoturvariskit ovat ja miten ne voivat vaikuttaa sekä yrityksen että hänen oman elämänsä toimintoihin.

Riskienhallinta on järjestelmällistä yrityksen toimintaan vaikuttavien uhkatekijäiden tunnistamista ja niiden varalta valmistautumista. Kaikkia riskejä ei saada poistettua, joten yrityksen johdon tulee määritellä taso, jossa riskit ovat hyväksyttävissä. Näin ollen tehdään riskienhallintapolitiikka, riskien torjumiseen ja hallintaan soveltuvat menetelmät, vastuutetaan ja suoritetaan tehtävänanto eri toimijoille yrityksessä sekä luodaan seuranta- ja raportointimenetelmät sekä -käytännöt. Riskienhallinta on prosessi ja sen tulee olla osa yrityksen johtamiskulttuuria ja -menetelmiä.(ICT Standard Forum, 2019c). Tietoturvallisuuden kautta pyritään estämään yritykseen kohdistuvia uhkia ja sitä kautta riskejä. Tietoturvan riskienhallinta vaatii jatkuvaa tietoturvan kehittämistä ja yrityksen toimintaan kohdistuvien uhkien tiedostamista. Hyvä valmistautuminen tietoturva-asioissa edesauttaa yritystä riskienhallinnan osalta. Tietoturvakulttuurin kasvattaminen ja kehittäminen ennakoi varautumaan mahdollisiin riskeihin hyvissä ajoin. Tästä syystä on merkityksellistä, että tietoturvakulttuuria kehitetään jatkuvasti ja oma henkilökunta pidetään valveutuneena uhkien varalta. Tietoturvan riskienhallinta vaatii kuitenkin jatkuvaa johdon huomiota, sillä tekniikka muuttuu jatkuvasti ja uhat leviävät eri reittejä myöden. Yritysten tietojärjestelmät ovat jatkuvasti erilaisten toimijoiden negatiivisen toiminnan kohteena.(Kansainvälinen Kauppakamari, 2019) Näin ollen tietoturvaan liittyvät arvioinnit ja prosessit kannattaa ulottaa sovellustoimittajiin asti. Toisiinsa liitetyt järjestelmät saattavat sisältää heikkoja kohtia, joita vihamieliset toimijat etsivät. Heikkoihin kohtiin kuuluvat niin tekniikka kuin ihmiset. Huolimatta järjestelmällisestä ja selkeästä viestinnästä, huonoja uutisia tulee ja niiden käsittely saattaa toisinaan olla vaikeaa (Kansainvälinen Kauppakamari, 2019).

Riskienhallinnan tietoturvariskejä tulee arvioida säännöllisesti, esimerkiksi puolen vuoden välein sekä uusien järjestelmien hankintavaiheessa ja vaikuttavien muutosten yhteydessä. Tietoturvan riskienhallinta on osa yrityksen riskienhallintaa ja sitä varten tulisi olla riskienhallintaryhmä, joka arvioi riskien vaikutuksen liiketoimintaan sekä päättää hallintakeinoista, joilla riskit saadaan minimoitua. (Teosto, 2018)

Yhteenvetona, tärkeitä askelia riskienhallinnassa ovat (Kansainvälinen Kauppakamari, 2019):

- tehdään organisaation riskianalyysi ja sitä kautta riskien priorisointi
- käynnistettävä toimet parhaiden tietoturvakäytäntöjen noudattamiseksi
- varautuminen tietoturvahäiriöiden havaitsemiseen prosessinomaisesti

Ensisijaisesti riskejä tulee välttää, toissijaisesti tulee minimoida niiden aiheuttama uhka. Mahdollisia vahinkoja pyritään rajoittamaan. Hyvä ennakkosuunnittelu edesauttaa vahinkojen korjaamisen nopeutta ja tarkkuutta. Sähköisten uhkien kohdalla turvatoimet voivat olla jopa parempia kuin uhka edellyttää. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2001b). Seuraavassa alaluvussa esitellään niitä periaatteita, joilla tietoturvan riskienhallintaan vaikutetaan.

2.3.1 Turvatoimenpiteitä tietoturvauhkiin varautumiseen

Markkinoilla on lueteltu lukuisia erilaisia toimenpiteitä, joiden avulla voidaan varautua tietoturvaloukkauksiin ja -uhkiin. Kohdeyrityksen toimenpidelistalta löytyvät useat luetelluista asioista.

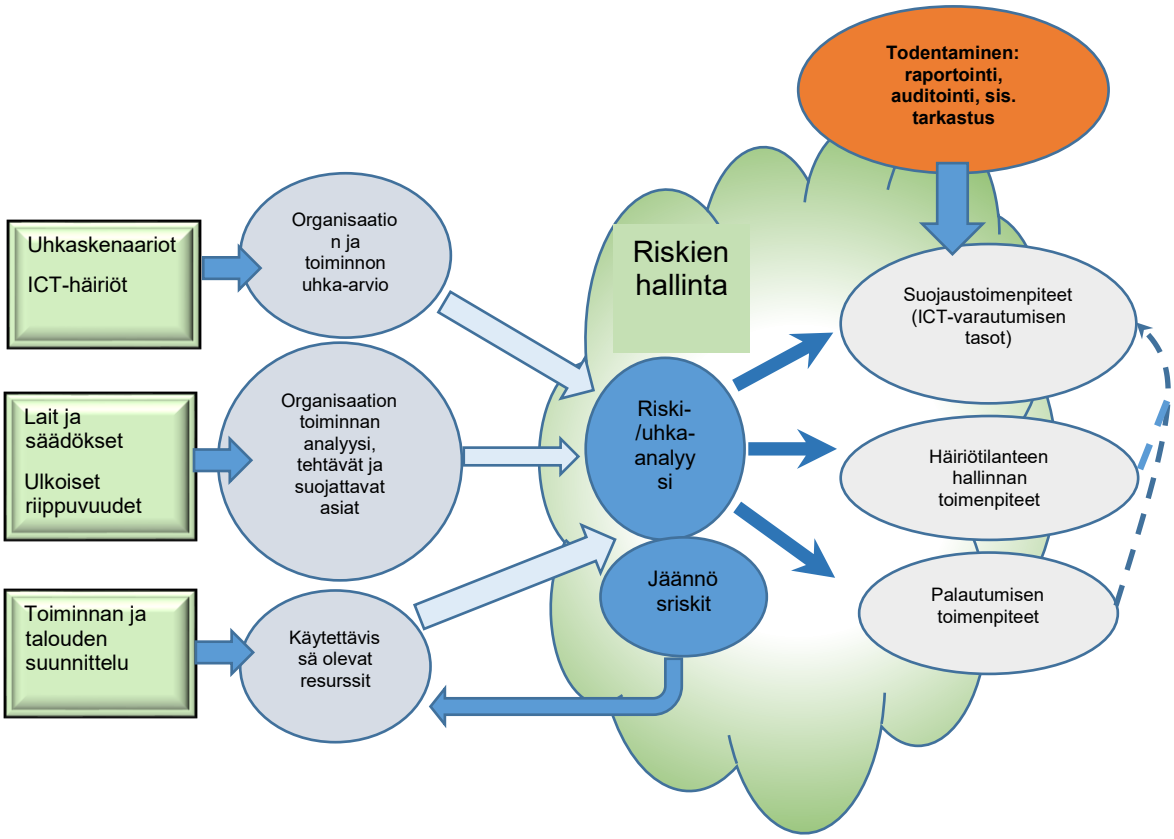
Yrityksen tietojen sekä järjestelmissä olevien tietojen suojaus lähtee liikkeelle varmuuskopioinnista. Varmuuskopioinnin tulee olla säännöllistä, riittävän pitkäaikaista ja suojattua, jotta tieto on tallessa eheänä, luotettavana ja se on helposti saatavilla yrityksen omaan käyttöön. Usein varmistusmenetelmiin liittyvät laitteistot ovat helposti mukana kuljetettavia, jolloin erityisesti niiden fyysinen turvallisuus tulee taata. (Kansainvälinen Kauppakamari, 2019) Sovellusten ja järjestelmien sekä laitteistojen päivitykset on huolehdittava ajanmukaisesti. Tietoturvapäivitykset tulee suorittaa mahdollisimman pikaisesti siitä, kun sellainen on saatavilla. Automaattipäivitykset auttavat tässä työssä ja näin voidaan varmistaa päivitysten oikea lähde. (Kansainvälinen Kauppakamari, 2019)

Tietoturvaperehdytykset sekä koulutukset ovat tärkeä osa tietoturvaa. Kaikilla yrityksen henkilöillä tulee olla omaan tehtävään soveltuva, tietoturvallisuuden toimien ymmärrystä tukeva, koulutus. Henkilöstön vastuu hallussaan olevista tiedoista ja niiden suojauksesta tulee olla selkeää.(Kansainvälinen Kauppakamari, 2019) Kohdeyrityksessä koulutukseen perehdytään tämän työn kautta tarkemmin ja luodaan samalla omaa tietoturvakulttuuria sisäisille käyttäjille.(Kansainvälinen Kauppakamari, 2019)

Tietoympäristön valvontaan on käytettävissä erilaisia tunkeutumisenesto -järjestelmiä sekä turvallisuushäiriöiden hallintajärjestelmiä. Niiden tuottamien tietojen jatkuva seuranta sekä analysointi yhdessä sovellusten kanssa antaa laajemman kuvan turvallisuudesta. (Kansainvälinen Kauppakamari, 2019) Kohdeyrityksessä on hiljattain tehty sopimus ulkopuolisen toimijan tuottamasta palvelusta, jotta tietoturvallisuutta kyetään hallinnoimaan paremmin myös teknisesti (Jansson, 2019b). Yritys voidaan suojata monikerroksisella suojauksella. Tällä tarkoitetaan viruksilta, haittaohjelmilta tai haittaohjelmalaitteilta ja hakkereiden hyökkäyksiltä suojautumista useiden laite- ja ohjelmistoratkaisujen avulla. Näin voidaan estää tai vähintään rajoittaa tietoturvaloukkausten vaikutuksia.(Kansainvälinen Kauppakamari, 2019)

Riskienhallinnalla pyritään minimoimaan syntyviä haittavaikutuksia. Riskienhallinta tarkoittaa siis, että yrityksellä on resurssit toimia nopeasti hyökkäyksiä vastaan, tietojen tallennus on huolehdittu ja mahdolliseen hyökkäykseen on varauduttu. Varautumisen avulla voidaan minimoida haitallisia tekijöitä. Organisaatiolla on suunnitelma, joka auttaa nopeiden päätösten tekemisessä ja mahdollistaa nopeat toimenpiteet. (Kansainvälinen Kauppakamari, 2019). Riskienhallintaa voidaan myös arvioida sisäisesti sekä ulkoisesti. Kohdeyrityksessä ovatkin käytössä riskienarvioinnin Tikka- sekä Kotka-arviointimenetelmät (Jansson, 2019b).

Kuva 4 kuvaa Valtionvarainministeriön riskienhallintaprosessia ICT-varautumisen näkökulmasta, VAHTI 8/2009 -ohjetta Tilannetietoisuudesta ja riskienhallinnasta (Valtionvarainministeriö, 2009) mukaisesti.



Kuva 4: Riskienhallintaprosessi ICT-varautumisen näkökulmasta (Valtionvarainministeriö, 2009)

2.3.2 Tietoturvariskienhallinnan turvallisuusperiaatteet

Yrityksen, sen työntekijöiden ja sidosryhmien tietoturvan suojaamiseksi toimintaan liittyy toimintamalleja, joiden avulla voidaan varautua ja torjua turvallisuusriskejä. Toimintamallien jatkuva kehittäminen parantaa yrityksen mahdollisuuksia kohdata tietoturvariskejä. Yhteisellä tietoturvakulttuurilla yritys toimii vahvasti niitä kohdatessaan. Kulttuuria voidaan vahvistaa yhteisillä toimintamalleilla ja jokaisen työntekijän huolellisella perehdytyksellä.

Tietoturva ei ole ainoastaan tietotekniikkaa tai teknisiä välineitä. Ajattelumalli tietoturvasta lähtee jo yritysjohdon ajattelusta ja suuremman kuvan näkemisestä. Kysymys on toimintaprosessista, joka koostuu ihmisistä, prosesseista ja tekniikan kokonaisuudesta. Näin ollen toiminnassa ovat mukana mm. järjestelmät, tekniset ratkaisut, laitteet, tietoverkot, toimintatavat, ihmiset ja moni muu yrityksen toimintaan liittyvä asia. (Kansainvälinen Kauppakamari, 2019) Tietoturvan ja em. asioiden kokonaisuudesta puhutaan nimityksellä Kyberturvallisuus (Vähänen-Koivuluoma, 2018). Ihminen on edellä mainituista tekijöistä tärkein osatekijä. Jopa 35 prosenttia tietoturvahäiriöistä aiheutuu ihmisen inhimillisestä toiminnasta. Nimenomaan tähän voidaan vaikuttaa onnistuneella koulutuksella ja perehdytyksellä. Loppu 65 prosenttia

koostuu varsinaisista hyökkäyksistä, mutta siitäkin osa olisi voitu välttää tiedon turvallisemmalla käsittelyllä. (Kansainvälinen Kauppakamari, 2019)

Toisinaan kuitenkin tapahtuu häiriöitä, varsinkin silloin, kun lakien ja säädösten vaatimat toimet on tehty ja ote herpaantuu. Odottamaton hyökkäys yllättää toimintaprosessit uhan ollessa nopeasti muuttuva, eikä siihen ole vielä osattu varautua. Toimintaprosesseja ja varautumista tietoturvauhkiin tulee siis päivittää usein ja niiden riittävyyttä tulee arvioida. Näihin arviointeihin voidaan käyttää sisäisiä ja ulkoisia auditointeja, joissa testataan mm. tunkeutumisen havainnointia. Tietohallinto ei yksin vastaa näistä toimista, vaan muiden sidosryhmien tulee osallistua ongelmatunnistukseen sekä tietoturvan jatkuvaan ja pitkäkantoiseen suunnitteluun. Yrityksen tulisi kasvaa tietoturvalliseen ajattelutapaan, jolloin myös uusien tietojärjestelmien suunnitteluvaiheessa otetaan huomioon niiden turvallisuus sekä palautukseen ja hyökkäysten torjuntaan kuuluvat toiminnot jo ennen järjestelmän käyttöönoton toteutusta. Tietohallinnon tulee siis olla mukana toiminnassa heti alkuvaiheessa. (Kansainvälinen Kauppakamari, 2019)

Tietoturvaloukkaus tulee tapahtumaan, aika vain ei ole tiedossa. Kun näin käy, onko yritys valmiina? Yritysjohdon vastuulla on tietoturvaloukkauksia kohdatessaan olla varautunut varautumissuunnitelmalla. Pelkkä suunnitelma ei riitä, vaan on oltava myös teknisiä vastatoimia. Suunnitelmassa tulee olla määriteltyinä tunnusmerkit, jotka osoittavat ulkopuolisten asiantuntijoiden avuntarpeen ja tarvitaanko esimerkiksi viranomaisten apua tilanteessa. Osa loukkauksista vaikuttaa yhteiskunnalliseen uhkaan ja tästä syystä vaativat ilmoitusta viranomaisille. Varautumissuunnitelma sisältää myös sisäisen ja ulkoisen viestinnän suunnitelman, jonka noudattaminen on tärkeä osa avoimuutta. Varautumisessa kannattaa tehdä myös vertaistyötä muiden vastaavien yritysten kanssa. (Kansainvälinen Kauppakamari, 2019) Tietoturva vaatii yritysjohdon sitoutumista ja sen osoittamista. ”Mitä isot edellä, sitä pienet perässä” toimii tässäkin. Yritysjohdon toiminta on esimerkki yrityksen henkilöstölle. Varsinaiset tekniset toiminnot suorittaa kuitenkin Tietohallinto-osasto, joka raportoi tietoturvatoimien vaikuttavuudesta sekä niiden riittävyydestä yrityksen johdolle. Raportointia on hyvä tehdä tämän lisäksi johtoryhmälle, tilintarkastajille sekä hallitukselle. (Kansainvälinen Kauppakamari, 2019)

Kohdeyrityksen tapauksessa ICT-jorylle raportoidaan toimista ja tietoturvauhkien tilanteesta maailmalla kuukausittain (Jansson, 2019b). Kohdeyrityksessä noudatetaan johtoryhmän ohjeistuksia (Pori Energia Oy Johtoryhmä, 2019). Tietoturvapolitiikka on tietoturvallisuuteen liittyvien toimintatapojen sekä niiden suositusten ja standardien kokoava dokumentti. Tämän rinnalle yrityksen kannattaa rakentaa visio siitä, mihin yritys on tietoturvan suhteen menossa ja millaisia turvallisuusvaatimuksia sillä on mm. ulkopuolisiin toimijoihin. Ulkopuolinen taho on aina riskitekijä. IT-palvelutarjoajien avulla voidaan parantaa yrityksen tietoturvariskienhallintaa sekä laitteistoja ja palveluita. (Kansainvälinen Kauppakamari, 2019). Tietoturvariskien hallinta on jatkuva ja kehittyvä prosessi, tästä syystä sen kehittäminen ja ajan mukana pitäminen on enemmän kuin tärkeää. (Kansainvälinen Kauppakamari, 2019). Tietoturvajohtamiseen kuuluu aina riskianalyysin perinpohjainen tekeminen (Pfleeger, Pfleeger and Margulies, 2003) Lähtökohtaisesti sen luomisessa on mietittävä yrityksen kokonaisturvallisuutta. Teknisesti se kannattaa tehdä kahdessa osassa, joista toinen on riskien kartoittamista ja toinen osa käsittelee niiden arviointia. Yleisesti ottaen systemaattisella riksikartoituksella pyritään selvittämään toimintaan liittyviä riskejä ja uhkakuvia. Niiden vaikutusta mitataan mittareilla, joiden kautta on mahdollisuus havaita eheydelle, käytettävyydelle ja luottamuksellisuudelle aiheutuvien vakavien vahinkojen

mahdollisuus (Hakala, Wuorinen and Vainio, 2006) Tietoturvallisuuden riskienhallinta pyrkii ennakoimaan ja näin eliminoimaan mahdollisia riskejä. Kaikkia ei kuitenkaan voida poistaa, mutta riskienhallinnan avulla syntyviä riskejä pyritään pienentämään siten, että ne voidaan hyväksyä. Erilaisten riskien ymmärtäminen ja niihin varautuminen sekä reagoiminen on osa tietoturvakulttuurin kehittämisen pääkohtia. Riskejä tulee arvioida myös sidosryhmiin kohdistuen. Riskien arvioinnin tulisi olla säännöllistä, jotta toimintaa voidaan kehittää. Toiminnan kehittäminen vaatii avointa tiedottamista sekä tietoturvariskien jatkuvaa raportointia. (Ruonala, 2011). Turvallisuusperiaatteiden ulottaminen jatkuvasti uusiutuviin järjestelmiin on osa tietoturvallisuuskulttuurin kehittämistä. Tietoturvan perehdytysohjelmassa tuleekin pitää mukana myös nykyiset ja tulevat pilviteknologiat huomioiva osuus.

2.4 Tiedon jalkauttaminen

Tietoturvakulttuurin kehittäminen ja sitä kautta henkilökunnan perehdyttämistapojen kehittäminen on osa tietoturvan jalkauttamisen askelia. Jotta on mahdollista löytää oikeita tapoja jalkauttamiseen, on ymmärrettävä ihmisen oppimiskyvyn mahdollisuudet ja rajoitteet. Seuraavissa kappaleissa 2.4.1, 2.4.2 ja 2.4.3 läpikäydään oppimisen lisäksi oppimiskulttuurin kehittämisen prosessia sekä muutosjohtamisen näkökulmaa.

2.4.1 Oppiminen ja ihmisen vahvuudet oppimistavoissa

Tietoturvakulttuurin kehittämisen olennaisena osana toimii ihmisen kyky oppia asioita ja tätä kautta kehittyä. Ihmisen oppimismetodien ymmärtämiseksi on työhön otettu mukaan oppimiseen liittyviä asioita, joiden kautta päästään oikean metodin löytämiseen työn aikana. Oppimisella tarkoitetaan asioiden omaksumista puhtaalla opiskelulla, harjoittelulla, tietoja ja taitoja hankkimalla, esimerkin ja kokemuksen perusteella (Kielitoimisto, 2020). Oppiminen tapahtuu erilaisissa asiayhteyksissä kuten yksin tai ryhmässä, hitaasti tai nopeasti. Siihen vaikuttavat mm. muistin aktiivisuus ja motivaatio, joka aktivoi oppimisen sekä tarkkaavaisuus, joka määrittelee oppimisen laajuuden. Tarkkaavaisuuteen vaikuttavat mm. oppilaan kartuttama kokemus, oppimistilanne sekä kuormitus, esimerkiksi työssä, oppimistilanteen aikana. Jos jokin näistä puuttuu, oppiminen pysähtyy. Kaikkien toiminta vaatii aktivoinnin, sosiaalisia suhteita, merkityksellisiä asiayhteyksiä sekä fyysisiä ominaisuuksia oppimiseen. (Huhtanen, 2017). Kohdeyrityksen jatkuva kuormitus erilaisten projektien kautta vaikuttaa ehdottomasti oppimiseen ja asioiden sisäistämiseen, joten perehdytystavan tulee olla oppimista helpottava, motivoiva ja mielenkiintoinen.

Oppimisen tarpeet saattavat olla erilaisia, samoin opetettavan henkilön lähtökohta oppimiselle. Myös tavoite voi olla erilainen henkilöstä riippuen. Oppimista voivat häiritä erilaiset tunneperäiset asiat, kuten virheiden havaitseminen ja niiden tunnistaminen ja sitä kautta syntyvä psykologinen huonovointisuus. Ihminen kokee olevansa epämukavuusalueellaan. (Koivukunnas, 2018) Esimerkkeinä kohdeyrityksessä ovat uusien sovellusten käyttöönotot, osalle oppilaista motivaatio oppia on korkealla johtuen heidän roolistaan tietojärjestelmän käytössä. Toiselle taas oppiminen ei ole niin tärkeää, koska kokee, ettei tule käyttämään järjestelmää kovin syvällisesti. Tässä tilanteessa kouluttajan rooli voi olla vaikea, sillä motivaatio tulee pitää sopivalla tasolla huolimatta kohderyhmästä. Kokenut kouluttaja voi panostaa koulutustilaisuuteen oman

osaamisensa ja kokemuksensa sekä keräämänsä taidot ja tiedot. Hän voi kannustaa ja tukea oppilaita sekä auttaa eteenpäin valintojen tekemisessä (Koivukunnas, 2018). Kohdeyrityksessä sovellusten käyttöönotoissa kouluttajat ovat usein projekteissa mukana olleita ydinhenkilöitä, joiden vastuulla on niin kannustaminen ja motivaatio kuin itse sovelluksen opettaminen, joka on yleensä helpoin osa. Kouluttajasta riippuen koulutustavat vaihtelevat, mutta antavat mahdollisuuden myös yhteiselle oppimiselle. (Ristolainen, 2020)

Tietoturvan jalkauttamista henkilöstölle vaikeuttaa ihmisten erilaisuus vastaanottaa tietoa ymmärrettävästi. Tästä syystä onkin tärkeää hakea erilaisia oppimiseen vaikuttavia menetelmiä, jolla tiedon sisäistäminen on jokaiselle mahdollista. Kukaan ei kuitenkaan opi vain yhdellä tavalla, vaan ensisijainen tapa vaatii toissijaisen oppimistavan. Oppimistyylillä tarkoitetaan henkilön tapaa oppia uutta ja vaikeaa tietoa. Se sisältää tavan omaksua, käsitellä ja säilyttää tietoa muistissa. Oppimiseen vaikuttaa henkilön persoona, motivaatio ja emootio. (Tuomola, Maijanen and Prashnig, 1999b) Kohdeyrityksen henkilöstö huomioiden, on tietoturvan perehdytysmenetelmien määrä rajallinen. Eräs tyypillinen tapa on esittävä opetus, joka soveltuu hyvin tiedon jakamiseen sekä asioiden kuvaamiseen. Perinteisesti esittävä esitys on luento, esitelmä, puhe tai alustus, mutta se soveltuu hyvin myös etä- ja verkko-opetukseen (Vuorinen, 2001) Kohdeyrityksen henkilöstö sijaitsee hajallaan Porin ympäristössä sekä muiden maakuntien alueella, jolloin verkko-opetus on tavoiteltavin vaihtoehto. Verkko-opetuksen järjestämiseksi voidaan käyttää omia resursseja sekä ostaa, ainakin osa palvelusta, ulkopuolisilta palveluntarjoajilta.

Ihmisen oppimistapojen tunnistaminen voi olla vaikeaa. Kunkin henkilön tulisi tunnistaa oma oppimis- ja työskentelytapansa ja tietää omat heikot ja vahvat puolensa (Tuomola, Maijanen and Prashnig, 1999b). Tulee sallia myös epäonnistumisia sekä vahvistaa koulutettavien itsetuntoa antamalla palautetta. Opiskelu ei enää ole pelkästään suorittavaa oppimista. (Nygren, 2015) Haasteen tässä työssä tuo kohdeyrityksen henkilöstön määrä (noin 230 hlöä) ja jatkuva kiire heidän töissään. Eräänä menetelmänä aineistoissa mainitaan mielikuvittelu ja vastausten kerääminen (Koivula, 2019). Ihmisten jatkuva oppiminen on noussut entistä arvokkaampaan asemaan, sillä teknologiat kehittyvät, maailma globalisoituu,

ihmisen tulee sisäistää entistä enemmän ja lyhyemmässä ajassa kuin aiemmin. Se mihin aiemmin on opiskeltu tai millaisia kursseja työn ohessa suoritetaan, ei enää takaa, että saatu oppi on ajankohtaista ja tarpeellista työelämässä. Voidaan sanoa, ettei tutkintokeskeinen ajattelutapa enää toimi. (Järvilehto, 2019) Ammatillisten alojen oppilaitosten ja yliopistojen tuleekin varsin nopealla tahdilla kääntää opetuksen suuntaa, jotta koulutus pysyy nykyteknologian mukana. Tämän päivän työntekijät eivät enää ole 40 vuotta samassa yrityksessä, vaan tulevat vaihtamaan usein työpaikkaa ja näin ollen aiemmin ajateltu koulutusputkikaan ei enää näytä samalta, eikä palvele opiskelijoita. Tätä kutsutaan palikkamaiseksi rakenteeksi, jota pitää muuttaa enemmän omatoimiseen opiskeluun ja osaamisen hankkimisen suuntaan osana omaa arkea. Vanha elämänmittainen oppiminen on muunnettava enemmän elämänlaajuisen oppimisen malliksi. Tähän kuitenkin tarvitaan niin päättäjien toimia, rohkeutta ja omaa motivaatiota. (Järvilehto, 2019). Jatkuva oppiminen liittyy myös jokapäiväisiin rutiineihin, joiden aikana ihminen voi oppia. Esimerkiksi oppimista voi tapahtua bussipysäkillä odottaessa, jolloin oppimismateriaali on sijoitettu silmin havaittavaksi. Eri paikoissa tapahtuva mainonta ja

markkinointi, uutiset ja Youtube -kanava sisältävät jatkuvan oppimisen aineistoa. (Casual Learning, 2020).

Mikro-oppiminen on eräs tapa toteuttaa jatkuvan oppimisen mallia. Lyhyet tietoiskumaiset, jopa viihdyttävät ja visuaaliset sisällöt kiinnostavat enemmän ollessaan monisisältöisiä kuin yksi pidempi osio. Mikro-oppiminen sopii erityisen hyvin aikuisiässä oleville henkilöille, jolloin lyhyiden sisältöjen vuoksi itse sisällöt on mahdollista sovittaa oman päivän rytmiin. Näin oppimiskynnys madaltuu ja toisaalta, sisältöjä voi olla useita. Häiriöt työn suorittamiseen ovat tavanomaisia, jolloin pitkäjaksoinen oppiminen voi olla vaikeaa ja toisaalta, se vie aikaa varsinaiselta tuottavalta työltä. (Leino, 2019b) Kohdeyritykseen suunniteltava perehdytysaineisto tulee tukemaan lyhyitä oppimisen jaksoja, jotka kuitenkaan eivät ole yksinkertaistettuja. Looginen ja johdonmukainen perehdytysaineisto sekä asioiden toistot aikaansaavat luottamusta. Tämän aineiston pohjalta luotava perehdytysaineisto tulee kuitenkin pitää ajan tasalla, muokata sitä saadun palautteen pohjalta ja mahdollisesti voidaan kokeilla erilaista tapaa toteuttaa oppimisympäristö. Aineiston tekemisessä ja ylläpidossa tulisi muistaa kohdeyrityksen henkilöstön erilaiset oppimistavat, joskin suurin osa ihmisistä oppii parhaiten visuaalisuuden kautta, jota tässä valitussa perehdytystavassa myös painotetaan. Jo tehdessä oppimisaineistoa kannattaa miettiä sen muuntumisen mahdollisuuksia ja sitä kautta helpottaa seuraavaa luontia. Materiaali voi olla hauskaa, leppoisaa ja rauhallista, aiheuttaa hymyä ja olla jopa viihdyttävä ja tarinallinen, jolloin koulutettavien on entistä helpompaa oppia ja mukavaa tutustua aineistoon. (Leino, 2019b) Kannattaa kuitenkin muistaa, että hauskat viihteelliset koulutuspätkät eivät ole kaikki, vaan perinteisen tavan syventävää tietoa tulee säilyttää ja ylläpitää näiden rinnalla. Kohdeyrityksen toimintajärjestelmä M-files tarjoaa siihen erinomaisen työkalun. Nykyisen tavan ja uuden tavoitellun tavan yhteen nitominen vaatii prosessointia.

2.4.2 Oppimiskulttuurin kehittämisen prosessi

Uudenlaisen perehdytysmekanismin luomisprosessissa tulee ensin tarkastella kohdeyrityksen nykyistä tapaa toimia. Perinteisiä opetusmateriaaleja ovat PDF-materiaalit, PowerPointit, erilaiset tehtävät tunnilla tai kotona, luokkaopetus sekä sähköisten apuvälineiden kautta opetus. Opetusmateriaalin ja yleensäkin dokumentaation ylläpito on tärkeää, vähintään annetun palautteen perusteella sekä varsinaisen tiedon muuttuessa. (Järvilehto and Leino, 2019). Tyypillisin opetusmuoto monissa yrityksissä on ns. neuvotteluhuone -perehdytys, jossa kouluttaja näyttää kalvoja ja puhuu oppilaiden kuunnellessa. Paranneltu versio tästä on yhteinen tekeminen kouluttajan ensin näyttäessä, jonka jälkeen alkaa henkilökohtainen tekeminen työasemilla kouluttajan kierrellessä ja neuvoessa (Ristolainen, 2020). Nykyinen perehdytyksen toimintamalli ei täysin toimi ollessaan pääasiassa esitys, joka on läpikäytävä joko henkilökohtaisesti tai ryhmässä. Moni muukin asiaan liittyvä dokumentti on kirjallisina ja löydettävissä toimintajärjestelmästä, josta henkilökunta ei joko ehdi tai jaksa lukea pitkiä ohjeistuksia. Toisinaan myös materiaalien löytäminen tuottaa ongelmia. Näistä syistä tämän työn ohessa on pyritty löytämään erilaisia tapoja lähestyä loppukäyttäjiä. Periaatteena uuden perehdytyskulttuurin suunnittelussa on käytetty kirjallisuudessa esiintyneitä, jo hyviksi havaittuja, toimintaohjeita.

Oppimiskulttuurin vaiheet sisältävät erilaisia huomioitavia asioita, kuten kuinka koulutettavat oppivat nyt, miten he oppivat sekä millaista oppimismateriaalia heille tällä

hetkellä on tarjolla. Tätä kautta on mahdollista tunnistaa organisaation oppimisen heikkoudet ja vahvuudet sekä hyväksikäyttää uuden oppimisaineiston luonnissa nimenomaan vahvuuksia. Hyvin suunniteltu oppimisaineisto on pohja koko organisaation oppimisaineistolle salliessaan kaikille saman toteutustavan. Uuden perehdytysmateriaalin luonti on usein vaikeaa. Sen luonti kannattaa antaa alan ammattilaisille, joilla on siihen taito. (O'Neil Emma, 2019). Kohdeyrityksessä onkin hyödynnetty 2NS - Second Nature Securityn tietämystä sekä materiaaleja, jotka kohdeyritys hankki itselleen alkuvuodesta 2020 tämän työn toteuttamista ja jatkokehitystä ajatellen. Oppimisaineiston luomisen apuna toimivat mm. koulutusaiheiden ja palautteen kyselyt koulutettavilta henkilöiltä (O'Neil Emma, 2019). Edellä mainittuja noudattaen kohdeyrityksessä tehtiin tietoturvan lähtötesti, jotta saatiin selville, mistä aiheista ihmiset ovat huolissaan ja mitkä jo koulutetut ja tiedotetut asiat selkeästi kaipasivat lisää tietoa. Perehdytystapojen tulee myös olla selkeitä, yksinkertaisia käyttää sekä saavutettavissa lähes mistä tahansa paikasta ja olla ajasta riippumaton. Tietoturvan perehdytysaineisto tulee läpikäydä jokaisen uuden työntekijän kanssa, jotta siitä tulee tapa oppia. Samalla työntekijä sitoutuu paremmin yritykseen. Oppimisaineistojen läpikäyntiin tulee varata aikaa ja siihen tulee erityisesti rohkaista, vaikka projektit usein vaikuttavat ajankäyttöön. Perehdytykseen käytettävän ajan varaamiseen voidaan myös luoda oma mekanismi yrityksessä.

Oikean perehdytystavan selviämiseksi kannattaa myös kokeilla erilaisia perehdytysmetodeja riippuen tilanteesta, johon metodia haetaan. Oppimismateriaalien keskittäminen tulee tehdä yhteen paikkaan ja tehdä sen läpikäynnistä jokapäiväistä esimerkiksi keskustelujen ja jaettujen artikkelien kautta. Yhdessä oppiminen antaa usein enemmän työntekijöille kuin yksin oppiminen. Keskustelut, yhteinen ideointi, työnjako ja erilaisista näkökulmista keskustelu rikastaa oppimisprosessia. (O'Neil Emma, 2019) Voidaan myös hyödyntää esimerkiksi Teams -keskustelukanavia tähän tarkoitukseen (Jansson, 2019b). Ihminen ei opi, jollei hän tiedä mitä pitäisi oppia, joten erilaisista oppimismateriaaleista ja -ympäristöistä kannattaa puhua ja markkinoida niitä sekä tiedottaa yleisesti koko henkilöstölle koulutuksista. Tiedon jakamisesta kannattaa tehdä tapa. (O'Neil Emma, 2019) Tätä tapaa kutsutaan nimellä Wisdom of Crowds, johon liittyy ajatelma ryhmän viisauden olevan kollektiivinen mielipide eikä ainoastaan yhden asiantuntijan mielipide (Sheng Kung *et al.*, 2012).

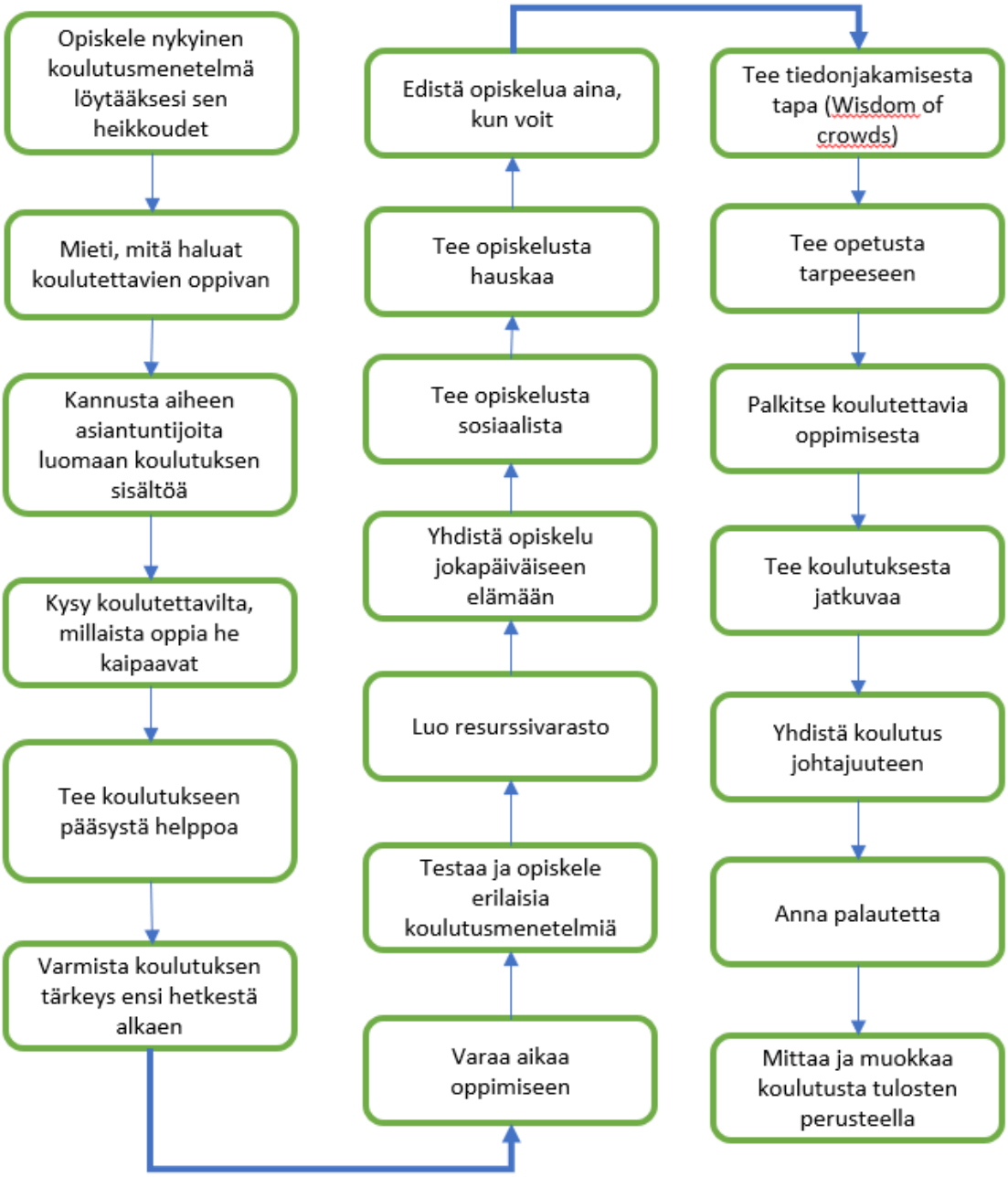
Kohdeyrityksen henkilöstö koostuu sekä toimihenkilöistä että työntekijöistä. Koko henkilöstölle on mahdollistettu erilaisten sähköisten välineiden käyttö, mm. kannettavat työasemat, yhteistyöasemat sekä erilaisia älymobiililaitteita. Näiden avustuksella verkko-opetusta voidaan organisoida koko henkilökunnan kesken. Yhtenä tavoitteena on saada henkilökunta toimimaan perehdytyksissä yhteistyössä, tukien toisiaan ja yhteisesti oppien. Puhutaan joukkoistamisesta ja yhteistoiminnallisesta työskentelystä eli ryhmässä työskentelystä. Ryhmän jokaisella jäsenillä on vastuu saavuttaa yhteiset tavoitteet. Yhteistoiminta ja yhteinen oppiminen on helpompaa, jos ryhmä on positiivisesti riippuvainen toisistaan – sen saavuttamiseen saattaa kulua aikaa, mutta tavoitteiden asettaminen auttaa edistymään. (Lavonen and Meisalo, 2003). Yhdessä työskentely ja toisten auttaminen ei aina työelämässä ole helppoa, koska ihmiset ovat erilaisia. Yhteistoiminnallinen työskentelytapa kuitenkin kehittää henkilöstön sosiaalisia taitoja ja lisäävät avointa vuorovaikutusta ryhmässä. ”Tieto on valtaa” ei enää toteudu, ennemminkin ”Yhteistyö on voimaa”. Kirjallisuudessa puhutaan myös sen kaltaisesta joukkouttamisen voimasta, jolla tarkoitetaan yhteisön osaamisen hyödyntämistä tiettyä

tehtävää ajatellen (Useita, 2018). Saatavat hyödyt liittyvät usein saavutetun tuloksen nopeuteen sekä edullisuuteen. Kohdeyrityksen henkilöstön monimuotoisuus edesauttaa kollektiivista ongelmanratkaisukykyä. Tuloksena työstä saatava hyöty kasvaa, toiminta tehostuu ja kustannukset vähenevät (Chanal and Caron-Fasan, 2010). Hyviä sosiaalisen median esimerkkejä Wisdom of Crowds -mekanismista ovat Wikipedia, Yahoo ja vastaavat sivustot, jotka nojaavat yhteiseen tietotaitoon. (Sheng Kung *et al.*, 2012). Kohdeyrityksessä sisäisessä ja jaetuin osin myös ulkoisessa viestinnän käytössä ovat Teams sekä jo aiempaa perua Slack, joiden kautta tietoa voi jakaa (Jansson, 2019b). Työn aikana uutena tiedon jakamiskanavana on yrityksen johdon toimesta, tietohallinnon tuella, otettu käyttöön myös Stream -videokanavat, jotka kuuluvat O365-perheeseen.

Oppimis- ja perehdytysaineistojen luominen perustuu usein tarpeeseen. Aineistoja tulee tehdä ja päivittää säännöllisesti, jotta sisältö vastaa tavoitteita ja on ajanmukainen. Oppimisesta kannattaa myös palkita jollain tavalla. Pelkkä maininta ja kehu voi jo motivoida, joskus jokin muu palkinto suorituksesta on motivoivampi. Samalla kouluttajat kokevat saavansa arvostusta tekemästään työstä. Hyvin yrityksen muuhun toimintaan nivottu oppimiskulttuuri takaa sen jatkuvuuden ja kehittymisen ja pitää sen mielenkiintoisena. Myös yrityksen johdon tulee osallistua perehdytyksiin ja sitä kautta nähdä sen merkitys yrityksessä. Muu henkilöstö seuraa johtajia. Perehdytyksistä ja koulutuksista tulee myös antaa palautetta oppimistilaisuuden jälkeen, jotta koulutettavalla on mahdollisuus oppia myös virheistään. Koulutettavien palaute on myös tärkeää, jotta perehdyttäjä voi oppia. (O'Neil Emma, 2019). Tästä syystä kohdeyritykselle luotava perehdytysaineisto sekä sen loppukysely sisältävät tietoa siitä, mikä meni oikein ja mikä väärin sekä antaa vastauksen kysymykseen kertauksenomaisesti.

Työn tarkoituksena oli tuottaa kohdeyritykselle perehdytysmateriaali, joka on kohdistettu tietoturvallisuuden tärkeimmiksi koettuihin osa-alueisiin. Materiaalin pituus tuli säilyttää riittävän lyhyenä, jotta koulutettavan kuluttama aika oli riittävän lyhyt sekä motivaatio säilyi läpi koko materiaalin. Lisäksi oli huomioitava materiaalin jatkuvuus ja uudistumiskyky. Materiaalin päivitys ei saa tuottaa liian suurta työtä ja sen tulee pysyä ajantasaisena sekä mielenkiintoisena pitkään ensimmäisen vaiheen jälkeen. Tarkoituksena oli suunnata perehdytystapaa ja -kulttuuria jatkuvan oppimisen mekanismeihin sekä hyväksikäyttää oppimiskulttuurin luomisen uusimpia mekanismeja. Mittareiden luonti oppimisympäristöille kannattaa ehdottomasti tehdä esimerkiksi työn jälkeisenä toimintona, sillä niiden avulla voidaan mitata koulutettavien sitoutumista, suorittamisen tasoa, koulutuksen onnistumista ja muita vastaavia asioita (O'Neil Emma, 2019). Mittaamalla voidaan myös löytää palkitsemisen ansaitsevia henkilöitä tai ryhmiä.

Kuva 5 esittelee erästä kirjallisuuden prosessia, miten oppimis- tai opettamiskulttuuria voidaan lähestyä. Kyseinen tapa esittelee 20 vinkkiä lähestyä opetusaineistoa siirryttäessä vanhasta koulutusmenetelmästä uuteen koulutusmenetelmään. Mekanismi kannustaa mikro-oppimisen menetelmiin (O'Neil Emma, 2019).



Kuva 5: 20 TIPS for creating a learning culture in the workspace (O'Neil Emma, 2019))

Kohdeyrityksen perehdytyskulttuurin rakentamisessa on huomioitava kiireinen teknologian uudistuminen, yritysmuutokset sekä luonnollisesti tietoturvaan kohdistuvat hyökkäykset, jotka vaikuttavat kiihtyvän. Tietoturvaperehdytyksen tulee palvella kohdeyrityksen tarpeita, joten on otettava huomioon mm. sen suorittamiseen mahdollistavat laitteistot sekä ajankäyttö. Mikäli perehdytys vie paljon aikaa, sitä ei ole helppo järjestää. Ryhmämäinen perehdytys on usein vaikeaa järjestää monien ihmisten samanaikaisen aikaikkunan vuoksi. Tästä syystä perehdytykseen haettiin uutta, helppoa mallia, joka mahdollistaa myös omaehtoisen opiskelun arkipäivässä ja joka tukee jatkuvaa oppimista. Oppimisen kokonaisuutta ajatellessa jatkuva oppiminen vaikuttaa hyvin realistiselta tavalta oppia ja opettaa, joten siihen tulee perehtyä enemmän.

2.4.3 Muutosjohtaminen

Kohdeyrityksessä tapahtuva nopea teknologian kehittyminen vaatii työntekijöiltään notkeutta ja nopeutta. Tämä tarkoittaa myös, että oppimisen menetelmät sekä kulttuurin kehittäminen vaativat pieniä, mutta jatkuvasti tapahtuvia muutoksia. Nämä vaativat jatkuvaa opettelua, jotta henkilöstö sopeutuu rytmiin. Jatkuva oppiminen edellyttää, että henkilökunnan muutoskyky sekä luovuus kiihtyy aiempaan verrattuna. Mikä aiemmin oli hyvä tapa toimia, ei enää olekaan ehkä paras mahdollinen, vaan toimintatapoja ja prosesseja tulisi arvioida ja rohkeasti myös kehittää tuottamalla esimerkiksi uusia työkaluja omaan toimintaan. Kysymys on jatkuvasta muutoksesta, ei pelkistä projektiluontoisista pyrähdyksistä. Oppi avaa tien muutoksille ja aikaansaa helpommin uusia innovaatioita. Tämä ei kuitenkaan tapahdu ilman ponnisteluja, sillä muutoskyvyt vaativat jatkuvaa oppimista. Jatkuva oppiminen lähtee liikkeelle oppijoiden analysoinnista, jossa selvitetään mitkä asiat heitä kiinnostavat ja motivoivat (Järvilehto and Leino, 2019). Muutoksissa tuleekin huomata hyvin organisoitu muutoshallinta. Tietoturvauhkien jatkuva kehittyminen vaatii nopeaa toimintaa ja yrityksen toiminnan kannalta se on välttämätöntä. Uhkien jatkuvaa torjuntaa ja sen menetelmiä ohjataan yrityksen johdon antamin roolituksin (Pori Energia Oy Johtoryhmä, 2019) sekä tietohallinnon toimien kautta, näistä jälkimmäinen toimii tietoturvan ydinryhmänä. Tietoturvastrategia ja -politiikka kertovat yrityksen tavoitteista ja toimintojen kehittymisestä avoimesti kaikille niin toimintajärjestelmän kuin Teams -viestinnän avulla. Kaikilla yrityksen työntekijöillä on mahdollisuus osallistua keskusteluun. Kohdeyritys pyrkii näin tekemään muutoksia yhteistyössä ja avoimesti, jotta kaikilla olisi tarvittava tieto olemassa.

Perehdyttävän organisaation tulee kehittää kohdeyrityksen henkilöstölle monipuolinen oppimismenetelmä (Tuomola, Maijanen and Prashnig, 1999b). Tähän pyritään tekemällä työn aikana ns. LABS-kysely heterogeeniselle ryhmälle, joka edustaa henkilöstöä. LABS-kyselyn avulla pyritään kartoittamaan henkilöstön tapoja oppia asioita sekä motivoitua. LABS-kyselyiden kautta jatkojalostetaan menetelmät, miten erilaisia koulutusaiheita kohdeyrityksessä tullaan tulevaisuudessa jalkauttamaan (Niemi, 2020). Tavoitteiden saavuttamiseksi henkilöstön tulee tietää tavoite, mihin yritys pyrkii. Esittämällä konkreettisia tavoitteita selkeästi ja ymmärrettävästi sekä osittain myös viihdyttävin keinoin kuitenkaan ilman vitsejä, voidaan avata kuulijakunnalle muutoksen syyt sekä herättää motivaatiota. Oppimisen tulos itsessään merkitsee oppijalle – ”mitä tässä on minulle?”. Vastausten saamiseksi ensimmäisen perehdytyskierroksen yhteydessä kannattaa suorittaa perehdytystä koskeva testi, jolla pyritään saamaan lisätietoa perehdytyksen onnistumisesta. Näitä mekanismeja noudattaen perehdytyksistä voi tulla osa tietoturvakulttuuria.

Nykypäivän kiireisessä työmaailmassa on havaittu, että ns. mikro-oppiminen soveltuu hyvin aikuisten ihmisten opettamiseen. Mikro-oppimisella tarkoitetaan lyhyiden tekstien ja videoiden esittämistä pieninä annoksina. Paras oppiminen voidaan saavuttaa, kun oppimissisältöjä on lukumääräisesti paljon. Mikäli koulutettava tiedostaa, että opiskeluun kuluva aika on lyhyt, on motivaatio oppimistapahtuman suorittamiseen korkeampi. Oppimistapahtumat tulee usein suorittaa työpäivän keskellä pienissä aikaikkunoissa, jolloin lyhytkestoisilla sisällöillä saavutetaan enemmän kuin yhdellä pitkäkestoisella. Itse sisällön tulisi kuitenkin olla hyvä kokonaisuus ja asiallisesti laadukas, muttei mitenkään yksinkertainen. Mikro-oppiminen soveltuu vaikeasti ymmärrettäviin asioihin, mutta ei

kuitenkaan poista muita oppimismetodeja vaan toimii niiden täydentäjänä ja päinvastoin. (Leino, 2019a). Tänä päivänä puhutaan paljon myös pelillistämisestä opiskelutapana. Tämä tapa sopii hyvin monelle aikuisellekin, varsinkin kun motivaatio ja palkinto on kohderyhmälle mieluisa. Oppimismahdollisuudet kasvavat, kun opetukselle ja sen sisällölle on luotu malli. (Järvilehto and Leino, 2019) Tämän mallin avulla voidaan saavuttaa yrityksen konseptiin sopiva tapa toimia ja luoda perehdytyskulttuuri.

Tietoturvakulttuurin kehittämiseen ja sen osa-alueen, perehdytysmenetelmän löytämiseen ja jalkautuksen aikaansaamiseksi oli ymmärrettävä ensin, millaista kokonaisuutta on tarkoitus perehdyttää, miten ihmiset oppivat ja miten he toimivat parhaiten yhdessä, jotta oikea perehdytysmekanismi olisi löydettävissä. Samalla piti huomioida kohdeyrityksen strategiaan kuuluvat asiat, jotka toimivat työn ohjeena.

3. MENETELMÄT JA AINEISTO

Aiheen lähestyminen oli aluksi hankalaa. Tutkimusaiheen ymmärrys vei oman aikansa ja teoriallinen osuus tietoturvan osalta selkeytyi. Kuitenkin työn aikana ymmärrys ihmisen oppimistapojen ymmärtämisen tärkeydestä kasvoi ja lopulta hahmottuivat myös menetelmät, miten asiaa voidaan lähestyä. Seuraavassa olen esitellyt työn vaiheita ja lähestynyt niitä myös yksityiskohtaisesti.

3.1 Työn toteutusvaiheet

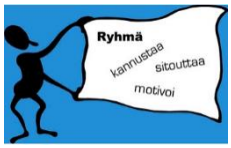
Työn suorittaminen huolellisen suunnittelun kautta teki siitä helpommin lähestyttävän kuin suora ajattelematon kirjoittaminen. Ensimmäisessä vaiheessa tuli määritellä työn tavoitteet ja kysymykset, joihin työn tuli vastata. Tämä työ lähti liikkeelle keväällä 2019. Teorian ja tiedon hankinta pystyttiin aloittamaan, kun työn tavoite kirkastui. Tavoitteeksi asettui tietoturvakulttuurin kehittäminen osa-alueenaan tietoturvan jalkauttamisen parhaat menetelmät kohdeyrityksen tarpeisiin. Kolmannessa vaiheessa avattiin O365-työvälineistä valitulla Teams -kanavalla tietoturva-asioiden tiedottaminen sekä keskustelut henkilökunnan kesken. Työtä varten läpikäytiin erilaisia sähköisiä perehdytysmenetelmiä. Lisäksi suoritettiin tietoturvan osaamisen selvitys yrityksessä ja saatujen vastausten analysointi. Tämä asettui ajallisesti loka-marraskuulle 2019. Neljännessä vaiheessa työn kirjoittaminen kiihtyi ja analyysit tuottivat oppimisen ydinalueiden selkeytystä. Motivointi Teams'in käyttöön lisääntyi talven aikana suoritettujen tiimiperehdytysten kautta. Viidennessä vaiheessa lopullinen perehdytystavan valinta vahvistettiin LABS-kyselyiden kautta pilottiryhmissä. Tämän lopputuloksena valittiin tietoturvallisuuden jalkauttamisen menetelmä ja aloitettiin materiaalin teko, johon hankittiin tukimateriaalia 2NS – Second Nature Security -yritykseltä. Lisäksi luotiin perehdytysten vuosikello. Viimeinen vaihe oli saattaa kirjoitustyö lopulliseen muotoonsa, jotta se vastaa työn perustavoitetta eli tietoturvakulttuurin kehittämistä perehdytystavan löytämisen avulla ja sitä kautta tietoturvallisuuden jalkautukseen kulttuuria tukevalla tavalla. Kuva 6 kuvaa lyhyesti työssä läpikäydyt vaiheet.

Vaihe 1: Aiheen suunnittelu sekä tavoiteasetanta, kevät 2019

Vaihe 2: Tiedon hankinta, 2019-2020

Vaihe 3: Tutustuminen sähköisiin perehdytysvälineisiin.
Tietoturvan osaamisselvitykset 10-11/2019 ja tulosten a**nalysointi**
Tietoturvatietoisuuden lisäys: tiedotus, keskustelu, toiminta Teamsin avulla

Vaihe 4: Analysointi ja tekeminen jatkuu
Perehdytysten erityisalueiden selvitys.
Teamsin käytön laajennus: motivointi ja tiedonjaon yhteisöllisyys (Wisdom of Crowds)



Vaihe 5: Tekeminen
LABS-kyselyt oppimistapojen selvittämiseksi.
Työn kirjoitus jatkuu.
Sähköisten opiskelumetodien sekä tiedonjako-kanavien valinta.
Tietoturvan perehdytysten vuosikellon luominen.

Vaihe 6: Materiaalin läpikäynti, tavoitteen kirkastaminen ja kirjoitetun materiaalin siivous maalis- ja huhtikuussa 2020.

Kuva 6: Työn etenemisen vaiheet

3.2 Yrityksen kuvaus ja konteksti

Pori Energia Oy:n historia alkoi 15.8.1898, kun kuopiolainen kirjapainoyrittäjä Otto Wilhelm Backman aloitti sähköliiketoiminnan Porissa. Yritys siirtyi Porin kaupungin omistukseen vuonna 1906. Sata vuotta myöhemmin vuonna 2006 Porin Kaupunki perusti Porin kaupungin Sähkölaitos -liikelaitoksesta osakeyhtiön, joka sitä kautta irrottautui Porin kaupungista omaa päätäntävaltaa käyttäväksi yritykseksi. Syntyneeseen osakeyhtiöön yhdistyi Porin Lämpövoima Oy. Porin Kaupunki omistaa 100-prosenttisesti koko osakeyhtiön.

Konserni koostuu kolmesta eri yrityksestä: Pori Energia Oy, tytäryhtiö Pori Energia Sähköverkot Oy sekä Tuulia Oy, joista viimeisellä ei ole vuonna 2019 ollut toimintaa. Henkilökuntaa konsernissa oli 231 henkeä vuonna 2019. Pori Energia -konsernin päätoimipaikka sijaitsee Porin kaupungin keskustan läheisyydessä, lähellä Karjarannan jokirantaa. Päätoimipaikassa työskentelee noin 100 työntekijää ja toimihenkilöä. Muu henkilöstö sijoittuu Porin kaupungin alueella Aittaluodon ja Kaanaan voimalaitoksille sekä tuulivoimapisteille Mäntyluodossa, Raahessa, Keminmaalla, Haukiputaalla ja Iissä. Pori Energia -konserni tuottaa ja tarjoaa asiakkaille erilaisia energiatuotteita ja -palveluita. Päätoimiala on sähkön ja kaukolämmön yhteistuotanto (Yritysrekisteri, 2018). Toiminta on vastuullista, lakien ja sääntöjen sekä lupausten ja sopimusten noudattamista samalla huomioiden oman toiminnan laadun merkitys sekä turvallisuus ja ympäristövaikutukset. Yrityksen asiakkaita ovat mm. tavalliset kotitalousasiakkaat,

taloyhtiöt, yritykset sekä teollisuusasiakkaat. Pori Energia Oy toimi vielä maaliskuussa 2020 noin 80 muun sähkönmyyntiyhtiön joukossa Suomessa. 1.4.2020 alkaen Pori Energia Oy sähkönmyynnin osuus yhdistyi viiden muun suomalaisen energiayhtiön kanssa. Näin yrityksen sähkönmyynti ja aurinkosähkötoiminta siirtyivät uudelle perustetulle yritykselle, Oomi Oy:lle. Pori Energia Oy:n omistus Oomista on 12.2 prosenttia.

Pori Energia Oy:n Energiapalvelut -yksikkö tuottaa kaukolämpöä ja -jäähdytystä sekä höyryä asiakkaidensa tarpeisiin voimalaitoksiensa avulla (Aittaluodon laitokset ja Kaanaan laitos sekä useita pienempiä kaukolämpökeskuksia). Lisäksi yritys tuottaa ja ylläpitää lämpöverkkoja niin Porissa kuin muutamissa ympäristökunnissa sekä Kristiinankaupungissa. Pori Energia Oy:n tekniset palvelut suorittavat kattavasti sähköjärjestelmien suunnittelua, katuvalaistuksen ylläpitoa ja kunnostusta, tietoliikennerakennusta sekä rakentamis- ja kunnossapitopalveluita. Lisäksi yrityksessä toimii hallinnollinen yksikkö sekä yrityksen toimintoja tukeva konsernipalvelut -yksikkö. Varsinaisia tuotteita ovat sähköntuotanto, kaukolämpö- ja jäähdytystuotteet, tuulivoimatuotteet, erilaiset sähkötekniset palvelut sekä tietotekniset palvelut asiakkaille kulutuksen seurantaan. Lisäksi Pori Energia tuottaa yhteistyössä kumppaneidensa kanssa sähköautojen latauspisteitä. (Markkinointi, 2018) Tytäryhtiö Pori Energia Sähköverkot Oy:n vastuulle kuuluvat mm. sähköverkkojen rakennuttaminen Porin alueella. Yrityksen vastuulle kuuluvat sähkön siirto sekä jakelu ja verkonhallinta. Yritys omistaa useita sähköasemia, yli tuhat jakelumuuntajaa sekä tuhansia kilometrejä sähköverkkoa.

3.2.1 Toimintaa kuvaavat tunnusluvut

Toimintaa kuvaavat tunnusluvut on kuvattu taulukossa 1. Tunnusluvut ovat vuodelta 2019 Pori Energian toimintakertomuksesta (Pori Energia Oy, 2019).

Taulukko 1: Pori Energia Oy -konsernintaloudellista toimintaa kuvaavat tunnusluvut (Pori Energia Oy, 2019)

Tunnusluku	Pori Energia Oy, konserni 2019	Pori Energia Oy, konserni 2018
Henkilöstön määrä, hlö	231	224
Liikevaihto, M€	141,5	138,3
Liikevoitto, M€	18,8	18,6
Liikevoitto/liikevaihto, %	13,3	13,5
Kannattavuus, ROI-%	6,6	7,4
Omavaraisuusaste, %	27,0	26,7
Investoinnit, M€	60,3	42,0

Taulukko 1 on nähtävillä esimerkiksi investointien kasvu verrattuna vuoteen 2018. Näitä ovat aiheuttaneet mm. Impolan sähköaseman saneeraus, sijoitukset sekä Aittaluodon uuden voimalaitoksen loppuvaiheen rakennuskustannukset.

Konsernin yhteiset arvot luotsaavat yhteiseen tekemiseen, joka on osa yhteisiä perehdytysmenetelmiä, avointa keskustelua ja tiedon jalkauttamista yritykselle soveltuvalla tavalla.

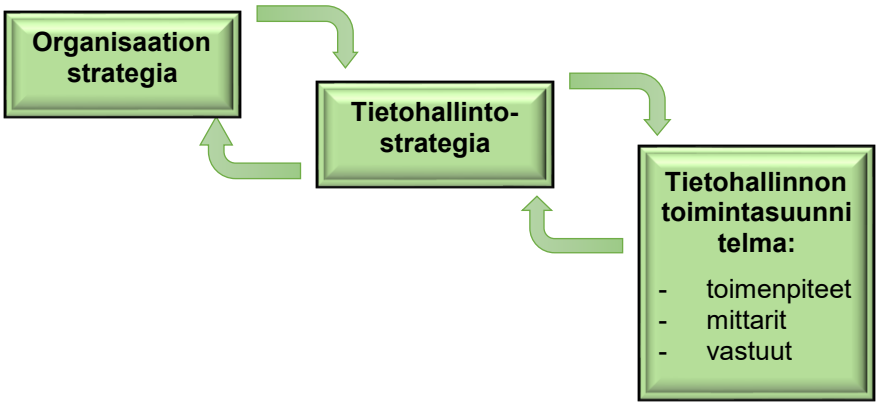
”Teemme työtä vastuullisesti, yhdessä toimien, asiakasta, työtämme ja toisiamme arvostaen sekä jatkuvasti toimintaamme kehittäen.” (Pori Energia Oy henkilöstö, 2020)

Yhteisiin arvoihin nojaten pyritään kohdeyrityksessä jakamaan ymmärrystä tietoturvan merkityksestä ja sen roolista yrityksessä.

3.2.2 Tietoturvan rooli yrityksen strategiassa

Tietoturvallisuuden rooli yrityksen strategiassa on merkittävä, jotta yrityksen toiminta on turvattua. Kaikkien työntekijöiden tulisi tästä syystä ymmärtää tietoturvan merkitys. Yrityksen strategiasuunnittelussa toimivien henkilöiden tulee olla tietoisia tietoturvan osuudesta. Tietoturvallisuuden perehdytysohjelmassa käsitellään lyhyesti myös tätä osaa turvallisuudesta.

Yrityksen strategian muodostuksessa tietohallinnolla on oleellinen rooli. Sen tulee tunnistaa organisaation eri toimijat sekä osapuolet. Vaateiden täyttämiseksi sen tulee olla aktiivisesti mukana koko yritysorganisaation suunnittelussa. Yhteisen suunnittelun kautta muodostuvat tietohallinnot omat tavoitteet. Suunnittelutyössä voidaan myös paremmin hyödyntää tietotekniikan mahdollisuudet ja nähdään niiden toteutuksen aiheuttamat resurssitarpeet. Kuva 7 esittää tietohallinnon strategian kehittymistä vuoropuhelulla liiketoimintaorganisaatioiden kanssa. (ICT Standard Forum, 2019a)



Kuva 7: Organisaation strategiasta tietohallinnon toimintasuunnitelmaan (ICT Standard Forum, 2019a)

Tyypillisesti yrityksen strategia sekä tietohallinnon strategia rakennetaan 3-5 vuoden ajaksi. Tietohallintostrategia paloitellaan kuitenkin tätä pienemmiksi aikayksiköiksi, jotta se palvelee organisaation tarpeita. Tavoitteet on asetettava yhdensuuntaisiksi organisaation strategisten tavoitteiden kanssa ja niiden toteutumisen varmistamiseksi. Liiketoimintayhteistyö yhdessä liiketoiminnan sekä tietohallinnon välillä on tunnistettava, jotta molemmat osapuolet toimivat yhdessä organisaationsa suunnittelussa. Yhteistyön avulla saadaan molemmille osapuolille toimivat tavoitteet sekä ymmärretään tietotekniikan tuomat hyödyt paremmin koko organisaatiossa. Strategisten pitkien aikajänteiden tavoitteiden saavuttamiseen vaaditut yrityksen liiketoimintakyvyt määritellään kokonaisarkkitehtuurissa. Sen tavoite on tuoda ratkaisuja liiketoiminnan tarpeisiin prosessien, sovellusten ja välttämättömien toimenpiteiden kautta. Mm.

yritysostot tai fuusiot, jotka ovat huomattavia muutoksia organisaatiolle, lisäävät haastetta kokonaisarkkitehtuurin joustolle. Kokonaisarkkitehtuurin tulisi olla myös luonteeltaan suhteellisen ketterä. Digitalisaatio ja sen lisääntyminen tekee arkkitehtuurisuunnittelusta haasteellista. (Business Technology Standard, 2020)

Kokonaisarkkitehtuurin hallinta energiayhtiön osalta on äärimmäisen tärkeää sen ollessa loppukäyttäjien eli asiakkaidensa perustarpeiden palveluntarjoaja. Näin ollen arkkitehtuurissa on välttämätöntä pitää kaikki julkisen verkon välityksellä tapahtuvat toiminnot täysin erillään organisaation omasta toiminnasta ja sen tietoliikenneverkoista. Näitä verkkoja ovat mm. Valvomoita koskevat verkkoyhteydet (sähköliikenteen ja –tuotannon hallinta) sekä muut niitä tukevat liiketoimintaverkot ja –sovellukset. Loppukäyttäjien palveluille sekä yrityksen internet –sivustoille tarjottavat palvelualustat tulee sijoittaa yrityksen verkon ulkopuolisille palvelimille. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2001a). Kokonaisarkkitehtuurin kankeus nähdään usein kuitenkin esteenä kehitykselle. Oikein laadittu arkkitehtuuri on kuitenkin joustava ja se taipuu nopeassa tahdissa digitalisaation tarpeisiin, kuten myös siitä aiheutuvan tietoturvallisuuden tarpeisiin. Yritykset sähköistävät digitalisaation avulla prosesseja, joihin tarvitaan sovelluksia. Jokaisessa sovelluksessa on tietoa ja näin kaiken tiedon hallintaan ja sovellusten väliseen tiedonvaihtoon tarvitaan integraatioita. Sovellusten ja integraatioiden toiminta vaatii IT-infran toimiakseen. Sen hallinnasta vastaa kokonaisarkkitehtuuri.

Hyvänä työkaluna koko organisaation synkronoimiseksi toimii aikataulutus sekä sen visuaalisena mallina yrityksen yhteinen vuosikello, johon tietohallinnon toiminta sovitetaan. (ICT Standard Forum, 2019c). Tietohallinnon strategiasuunnitelman ensimmäinen vuosi tulee tarkentaa yrityksen johdon kanssa yhdessä rakennettaessa toiminta- ja taloussuunnitelmaa. Jotta keskeiset tapahtumat ja niihin liittyvä muu toiminnan ajoitus on selkeästi seurattavissa, suosittelee tietohallintomalli näiden merkitsemistä vuosikalenteriin tai vuosikelloon toiminnan synkronoimiseksi sekä selkeän ja oikea-aikaisen tiedottamisen tueksi. (ICT Standard Forum, 2019a) Tietohallinnon johtamisen vuosikello tulee katselmoida vuosittain. Vuosikellon malli voi olla kvartaaleihin, kuukausiin ja jopa viikkoihin sidottu aikataulu, jossa huomioidaan yrityksen muut keskeiset toiminnot. Kuva 8 kuvaa esimerkkiä jonkin yrityksen vuosikellosta (ICT Standard Forum, 2019b). Vuosikelloon kannattaa liittää myös koulutuksiin liittyvät kuukausittaiset toiminnot.

Kuva 8: Esimerkkikuva tietohallinnon vuosikellosta (ICT Standard Forum, 2019b)

Vuosikello on osa kehittyvää ympäristöä ja näin ollen se muuttuu jatkuvan kehittymisen myötä joiltain osin. Muutosten perustana ovat vuosittain tarkasteltavat ja ylläpidettävät strategian tavoitteet sekä suunnitelmat. Usein strategiset muutokset ajoittuvat kevätkauteen. Tällöin syksylle ajautuvat uudet vuositavoitteet, joiden toimenpiteet suunnitellaan ja mitataan toteutumaa. Strategia on useamman vuoden mittainen, mutta budjetointi on kuitenkin vuosittaista. Kohdeyrityksessä tietohallinnon vuosikelloon on olennaista liittää osaston strategiatyö sen muihin tavoitteisiin ja suunnitelmiin, joihin myös tietoturvan perehdytys -ohjelma kuuluu. Näiden avulla voidaan nähdä suunniteltu kehityssuunta.

3.2.3 Kohdeyrityksen tietoturvapolitiikka

Jotta perehdytysmenetelmän valintaprosessin perusteet voisi ymmärtää, on ensin tiedettävä, millaisissa lähtökohdissa kohdeyritys oli ja millaisia strategia-ajatuksia yrityksellä oli ennen työtä. Kohdeyritys on luonut yrityksen strategian mukaisesti uuden tietoturvapolitiikan vuoden 2019 alussa (Pori Energia Oy Johtoryhmä, 2019). Politiikka toimii koko tietohallinnon ohjenuorana tietoturvatavoitteiden suhteen. Se myös määrittelee tietoturvan vastuuttamisen ja organisaation sitoutumisen tietoturvaan Kohdeyrityksen tietoturvapolitiikka noudattaa soveltuvin osin Valtiohallinnon tietoturvallisuusohjeita (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013).

Kohdeyritys on asettanut tietoturvatavoitteidensa saavuttamiseksi peruslinjauksia koskien niin henkilöstöä kuin sidosryhmiä. Näihin linjauksiin kuuluvat mm. ohjeistukset työvälineitä koskien sekä tiedon säilytykseen ja käsittelyyn liittyvät ohjeet. Tieto tulee

määritellä sovitun luokituksen mukaisesti. Kaikki yhtiön etua ja turvallisuutta vaarantava toiminta on kiellettyä ja yritykseen kohdistuvat tietoturvaloukkaukset toimitetaan poliisin tutkittaviksi. Tietoturvallisuutta ylläpitävät kriittiset toiminnot toteutetaan viipymättä. Myös sopimustoimittajien sekä yrityksen muiden sidosryhmien tulee sitoutua kohdeyhtiön tietoturvavaatimuksiin. Yhtiön käyttämä ja ylläpitämä toimintajärjestelmä sisältää tietoturvallisuuteen liittyviä toimintaprosessien sekä ohjeiden dokumentteja. Näiden tarkoituksena on varmistaa ohjeistusten riittävä mitoitus ja ajantasaisuus. Hallintaa parannetaan jatkuvan toiminnan kautta auditoinnein, saatujen palautteiden, innovaatioiden ja muiden havaintojen avulla.

Yhtiön tietoturvan hallintaan kuuluu useita osa-alueita, kuten tietoturvapolitiikka sekä sen tavoitteet ja toimintasuunnitelmat, tietoturvan organisointi roolitusten kautta, tietoturvakoulutukset. Henkilöstöturvallisuuden avulla pyritään varmistamaan henkilöiden soveltuvuus yhtiön palvelukseen. Tietoturvapolitiikan sisälle kuuluvat myös määritelmät pääsynhallinnasta eri tietoihin, toimitilaturvallisuus (kulunvalvonta), sidosryhmiin kohdistuvat turvallisuusnäkökulmat, luottamuksellisen tiedon salaus aitouden ja eheyden säilyttämiseksi. Käyttöturvallisuus huolehtii tietojenkäsittely-palveluiden toteuttamisesta asianmukaisesti, turvallisesti sekä häiriöttömästi sekä lisäksi on viestintäturvallisuus, jonka avulla varmistetaan tietoliikenneverkkojen ja tietoliikenteen turvallisuus ja häiriöttömyys. Tietoturvan hallintaan kuuluvat myös tietojärjestelmiin kohdistuvat mm. tieto- ja tuotantojärjestelmien hankinta-, kehitys- ja ylläpitotoimet, joiden avulla pyritään varmistamaan järjestelmien turvallisuus koko niiden elinkaaren ajan.

Yrityksen tietoturvan hallinnassa otetaan huomioon myös viestinnälle asetettavat vaatimukset. Näitä ovat tietoturvahäiriöiden hallinta, joiden avulla pyritään varmistamaan, että reagointi häiriöihin on johdonmukaista. Koska edellä mainituilla on vaikutus yrityksen toimintaan, on niistä viestittävä tarvittavin keinoin. Lisäksi kiinnitetään huomiota yhtiötä sääteleviin elimiin, mm. vaatimustenmukaisuuden kautta varmistetaan tietoturvallisuuden hallinnan yhdenmukaisuus säädösten sekä sidosryhmien vaatimusten kanssa ja jatkuvuudenhallinnalla, joka ottaa huomioon tietoturvan tavoitteet jatkuvuussuunnittelussa ja sen täyttymisestä. (Pori Energia Oy Johtoryhmä, 2019). Näiden lähtökohtien perusteella tarvitaan oikea ja tehokas tapa jalkauttaa yrityksen asettamia arvoja ja ohjeistuksia.

3.2.4 Tietoturvaan kohdistuvat roolit

Kohdeyrityksen tietoturvapolitiikka määrittelee tietoturvasta vastaaville toimille ja toimielimille vastuut tietoturvan ylläpidosta, kehityksestä ja toteutuksesta. Jotta yrityksen henkilöstöllä on ymmärrys tietoturvasta vastaavien henkilöiden rooleista, on tietoturvan sisäistäminen helpompaa. Vastuunjako yrityksessä on selkeä.

Toimitusjohtaja vastaa tietoturvan johtamisesti sekä vastaa siitä, että yhtiölle asetetut säädökset tulevat täytettyä. Hänen rooliinsa kuuluu luoda edellytykset tietoturvallisuuden suunnittelulle, toteutukselle sekä sen seurannalle ja päättää tietoturvan organisoinnista sekä sen linjauksista yhtiössä. Yhtiön johtoryhmä vastaa yhdessä valmius- ja varautumissuunnitelman laatimisesta sekä niihin liittyvistä suunnitelmista, raporteista, kehityskohteista ja ohjeistuksesta kuin myös yhtiön turvallisuudesta. Johtoryhmän toimiin kuuluvat em. käynnistäminen ja kehittäminen. Yhtiön valmiusjohtoryhmän

tehtäviin kuuluvat päättäminen ja tarvittavien toimenpiteiden käynnistäminen yhtiön toimintaedellytyksiä tai turvallisuutta vaarantavan kriisin vaikutusten torjumiseksi ja rajoittamiseksi. Valmiusjohtoryhmä myös tarvittaessa käynnistää toimenpiteet kriisitilanteesta palautumiseksi. ICT-johtoryhmän toimiin kuuluu yhtiön turvallisuuden sekä valmius- ja varautumistoiminnan suunnittelu, raportointi, kehittäminen ja ohjeistaminen. ICT-johtoryhmä saattaa em. kohteet käynnistykseen sekä valvoo niiden toteutumista. Se myös vastaa tietoturvamittareiden, raporttien ja sidosryhmä-palautteiden seurannasta ja käsittelystä sekä johdon katselmuksista ja muista riskienhallintapolitiikan asioista. ICT-palvelupäällikön rooliin kuuluu yhtiön sisäisen tietoturvatoiminnan ohjaus ja kehitys, huolehtiminen tietoturvan hallinnan dokumenteista, suunnitelman mukaisten sisäisten sekä ulkoisten auditointien järjestäminen ja sekä tieturvahallinnan raporttien valmistelu. Hän myös käsittelee tietoturvaan kohdistuvat poikkeamailmoitukset. (Pori Energia Oy Johtoryhmä, 2019)

ICT-tiimin tehtäviin kuuluu toiminnassa tapahtuneiden turvallisuuspoikkeamien yhteenveto. Tiimi seuraa tietoturvamittareita, valmistelee turvallisuusohjeita sekä edistää turvallisuustietoisuutta yhtiössä. Yhtiön johtajien, päälliköiden ja esimiesten vastuulle kuuluu tietoturva sekä sen tiedottaminen omassa tiimissä ja yksikössä. Henkilökunnan vastuulle kuuluu vastata omassa lähiympäristössään sekä työtehtävissään tapahtuvasta tietoturvallisuudesta sekä sille annettujen ohjeiden noudattamisesta. Jokaisen yhtiön palveluksessa olevan tulee informoida havaituista puutteista, poikkeamista tai läheltä-piti -tilanteista niin palautejärjestelmään kuin kiireellisissä tapauksissa suoraan ICT-palvelupäällikölle tai ICT-tiimille. Yhtiön sisäinen auditoija tekee arviointeja yhtiön turvallisuuden hallinnasta. Yhtiön tietojärjestelmillä tulee olla omistaja, vastuuhenkilö, käyttäjät sekä sen käytön ja ylläpidon henkilöstö. Omistaja vastaa siitä, että tietosuojaseloste ja tarvittaessa voimassaolevan henkilötietolain mukainen rekisteri-seloste ovat saatavilla kustakin järjestelmästä. (Pori Energia Oy Johtoryhmä, 2019)

Kohdeyrityksen roolitus on mittava, mutta tarpeellinen. Näiden roolien ymmärryksen kautta on henkilöstöllä tieto, kenen puoleen kääntyä, mikäli havaitsee yrityksen toimintaa uhkaavan tietoturvaloukkauksen tai muun toiminnan.

3.3 Sähköisten opetusmetodien kartoitus

Tietoturvan jalkautuksen tueksi työn aikana tutustuttiin sähköisten perehdytys-menetelmien tarjontaan. Markkinoilta on löydettävissä yrityksen johdolle ja tietoturvasta vastaaville henkilöille erilaisia maksullisia koulutuksia. Konsultointiyrityksiä on olemassa useita. Tarjontaa löytyy myös loppukäyttäjäkoulutusten järjestämiseen. Tässä työssä tutustuttiin lähinnä yritysten tarjoamiin sähköisiin perehdytystapoihin. Tarkasteluun valittiin energiayhtiöissä suosittuja palvelutarjoajia, jotka oppimisen lomassa samalla mittaavat oppimisen tasoa. Muiden vastaavien yritysten käyttö mahdollistaa vertailevan tiedon saannin kohdeyrityksen verkostojen avulla, mikäli vastaavia tarjokkaita päätetään käyttää.

Granite Partnersin Tietoturvakoulutus verkossa -järjestelmän (Granite Partners, 2019) kautta asiakkaan on mahdollista muokata kysymyksiä ja teoriaosuutta sekä halutessa lisätä siihen kuvamateriaalia. Tämä menetelmä voisi tukea nykyisen kirjallisen tietoturvaohjeistuksen jalkautusta. Palvelutarjoaja mahdollistaa kohdeyritykselle materiaalin jaon sille soveltuviin osakokonaisuuksiin. Ensimmäisessä vaiheessa

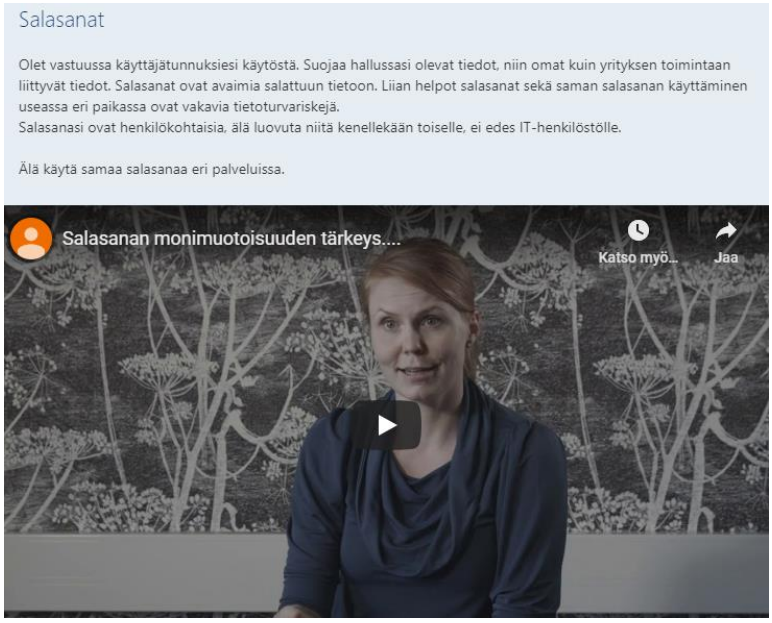
läpikäydään loppukäyttäjän perustietämys tietoturva-asioista, jonka jälkeen materiaalissa siirrytään opetuksellisiin osiin. Tentin suorittaneista käyttäjistä on saatavilla raportti.

Contrasec Oy tarjoaa erilaisia kursseja tietoturvavastaaville ja tietoturvapäälliköille sekä koko yrityksen tietoturvan kokonaisratkaisuja. (Contrasec Oy, 2019) Kurssit ovat yritykselle räätälöityjä kursseja, jotka usein pidetään paikan päällä, eivätkä näin ollen tarjoa verkkopohjaisia koulutuksia.

2NS - SECOND NATURE SECURITY OY Tietoturvapalvelut tarjoaa yrityksille tietoturvatestauksia sekä konsultointia. Tietoturvakoulutusta on tarjolla ohjelmistokehittäjille sekä yritysten henkilöstöille, jolle yritys on toteuttanut Kyberoppi-verkkokoulutuksen. (2NS - Second Nature Security, 2019) Yrityksen koulutus perustuu videoiden sarjaan, joissa läpikäydään erilaisia tietoturvatilanteita. Näihin on kytkettynä kyselyt. Yrityksen esimerkkivideon voi katsoa osoitteessa: https://youtu.be/0z3VfgclA_w. Myös 2NS tarjoaa käyttäjäraporttia tulosten analysointia varten.

Microsoft Forms on osa Microsoftin O365-sovellusperhettä. Se mahdollistaa yrityksen omatoimisen tietoturva –koulutusmateriaalin ja -tenttien luonnin. Järjestelmään voidaan lisätä kuvia, videoita, vaihtoehtoisia vastauksia, kirjallisia vastauksia, tähdityksiä ym., joiden avulla saadaan vastauksia loppukäyttäjiltä. Oikeat vastaukset voidaan liittää suoritukseen. Kyselyiden tuloksia voidaan analysoida, jolloin itsetehdyn perehdytyksen onnistuminen voidaan myös mitata. Kohdeyrityksessä Forms on käytettävissä yhtenä vaihtoehtoisena tapana tietoturvaperehdytysten luomiselle. Kuva 9 ja Kuva 10 esittävät kuva- ja videomateriaalinen liittämistä lomakkeelle.

Kuva 9: Esimerkki Forms'illa toteutettavasta kyselystä, jossa on kohdeyrityksen omaa aineistoa



Kuva 10: Esimerkki tekstin ja videon liittämisestä Forms'issa

Microsoft O365 Stream antaa lisävaihtoehtoja tarjoamalla mahdollisuuden tietoturvavideoille, joihin voidaan liittää Forms -lomakkeita tai -kyselylomakkeita, esimerkiksi kesken videon. Näin Stream mahdollistaa opin ja tentin samalla kertaa. Toisinpäin käännettynä Stream-videon voi liittää saman tuoteperheen Forms -lomakkeelle (kuten Kuva 10), jolloin asian keskelle voidaan asettaa esimerkinomaisesti video, joka kertoo tilanteesta.

Pohdintaa näiden vaihtoehtojen välillä aiheutti tietynlainen jäykkyys ostopaketeissa ja toisaalta O365-välineiden hybridi -mahdollisuus viehätti. Selvitysvaiheessa päätettiin hakea perehdytystavan valinnan vastausta viimeksi mainittujen kautta.

4. TULOKSET

Tietoturvan ymmärryksen nykykuvan sekä käyttäjien tietoturvaan liittyvien huolenaiheiden selvittämiseksi päätettiin ensin tehdä ns. Tietoturvallisuuden lähtökysely. Kyselyn onnistumista mitattiin ensin pilotoimalla. Tietoturvallisuuden lähtökyselyssä haluttiin ottaa käyttöön yrityksessä jo käytössä oleva O365 – perheen Forms-sovellus. Kysymyksissä hyödynnettiin aiemmin tietohallinnon sekä käyttäjien työssä eteen tulleita asioita ja aiheita sekä olemassa olevan tietoturvallisuuden perehdytysmateriaalin sisältöä. Tarkoituksena oli kartoittaa, mitä ihmisille on jäänyt mieleen aiemmista perehdytyksistä sekä tietoturvatiedotuksista, kuten myös toimintajärjestelmän ohjeista. Samalla pyydettiin valitulta pilottiryhmältä kommentteja heille esitettyyn kyselyyn sekä kehitystoiveita yleisesti tietoturvallisuusasioihin loppukäyttäjän näkökulmasta.

4.1 Tietoturvallisuuskyselyn pilotointi

Pilottiryhmään valittiin 50 käyttäjän heterogeeninen ryhmä, joista osa oli ns. peruskäyttäjiä ja osa edistyneempiä järjestelmien pääkäyttäjiä. Saatujen palautteiden pohjalta lähtökyselyä kehitettiin paremmin koko henkilökuntaa palvelemiseksi. Piloteille suunnattu kysely sisälsi seitsemän kysymystä tai toteamusta. Kysely oli tarkoituksella tehty lyhyeksi, jotta se oli riittävän nopea läpäistä eikä aiheuttanut liiallista mietintää vastausten suhteen. Valmiiden vastausten valinta viidessä ensimmäisessä kohdassa helpotti annettujen tulosten analysointia.

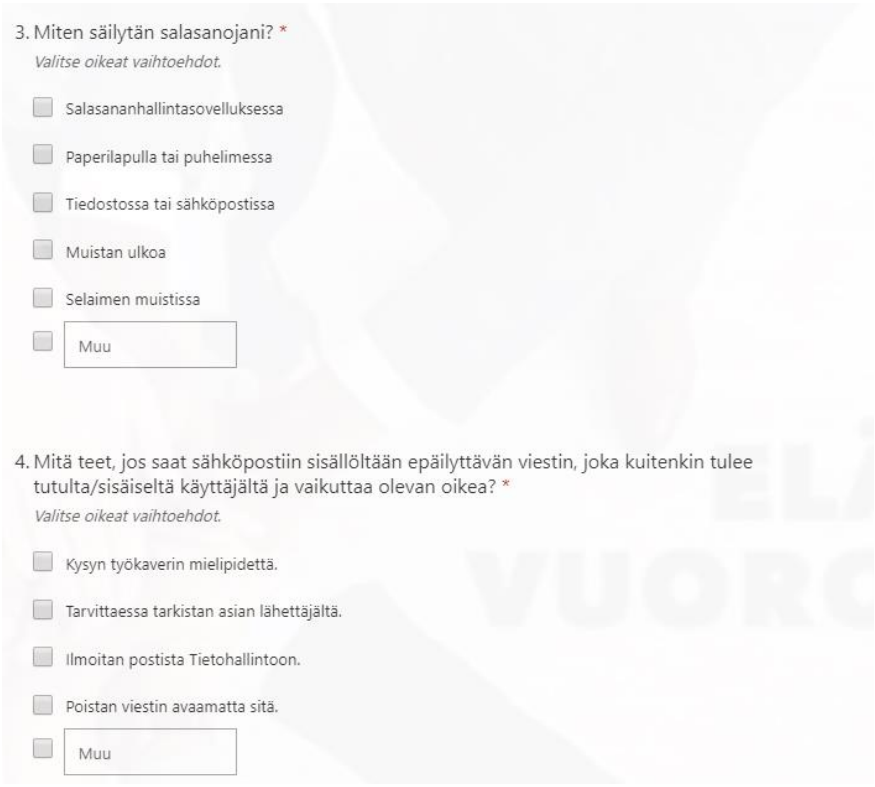
Kahdella ensimmäisellä kysymyksellä pyrittiin selvittämään, onko valittu kohderyhmä tietoinen yrityksen tietoturvapolitiikasta ja ovatko he tutustuneet yrityksen tietoturvaohjeisiin. Kysymyksessä kaksi otettiin huomioon myös se seikka, että ohjeiden sijainti ei olisi tiedossa. Tämä haluttiin asettaa kysymykseksi siitä syystä, että osaisimme myös parantaa ohjeiden sijainnin tiedotusta ja selkeyttää niiden löytymistä toimintajärjestelmästä.

Kyselyn sisällöt löytyvät seuraavista kuvista, Kuva 11, Kuva 12 ja Kuva 13.

Kuva 11: Tietoturvapolitiikan sekä tietoturvaohjeiden sijaintiin liittyvät kysymykset.

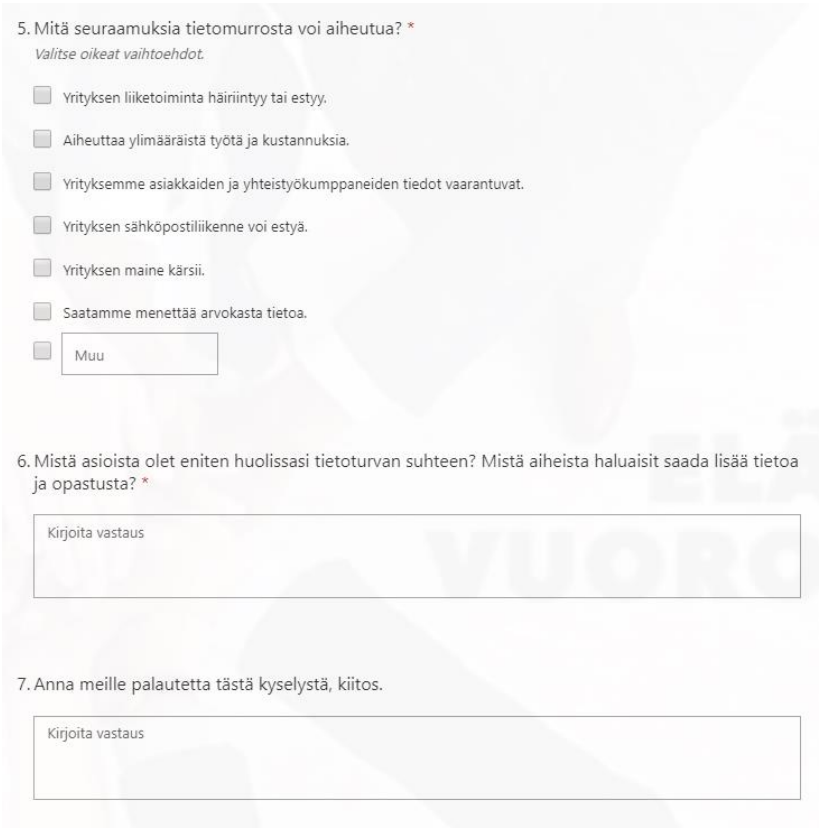
Alla olevassa kuvassa Kuva 12 on esitetty seuraavat piloteille suunnatut kysymykset. Kysymys kolme liittyy salasanojen säilyttämiseen ja hallintaan. Tämän kysymyksen tarkoituksena oli selvittää salasanahallintaohjelmiston tarvetta kohdeyhtiössä. Tietohallinto ei ole halunnut varsinaisesti suositella mitään sovellusta erikseen, mutta on varautunut ohjelman suositteluun. Kysymyksellä neljä haluttiin selvittää, mitä toimia

käyttäjät tekevät saadessaan jollain tavalla epäilyttävän sähköpostin. Tämä perustuu kohdeyrityksen tietoturvaviestintään ja sen ymmärrykseen näistä asioista.



Kuva 12: Alkukyselyn kysymykset 3-4.

Seuraavassa kuvassa, Kuva 13, kysymys viisi kohdistettiin vielä tietoturvanviestinnän aiheisiin, jossa haettiin ymmärrystä tietomurron seurauksista. Lisäksi esitettiin kysymykset kuusi ja seitsemän vapaan sanan muodossa. Näin haluttiin saada tietoa ihmisiä eniten mietityttävistä tietoturvallisuuteen liittyvistä asioista niin työssä kuin kotona. Piloteille suunnatussa kyselyssä myös palautteen antaminen kyselyyn oli tärkeää, jotta kyselyä pystyttiin jalostamaan varsinaista loppukäyttäjä -kyselyä ajatellen.



Kuva 13: Alkukyselyn kysymykset 5-7

Piloteista 34 vastasi kyselyymme, joka tekee vastausprosentiksi 68 prosenttia.

Lähtökyselyssä käytetty O365-perheen Forms -lomakesovellus mahdollistaa tietojen keruun suoraan taulukkonäkymään, jolloin tiedon jatkojalostus mahdollistuu. Lisäksi tulokset voidaan esittää graafeina, jolloin sen läpikäynti esimerkiksi eri työryhmissä on havainnollistavaa ja tarkasteltavissa visuaalisesti. Lähtökyselyn pilotoinnin jälkeen päätettiin lähestyä yrityksen muuta henkilökuntaa vastaavalla kyselyllä, jotta tietoisuus henkilökunnan tietoturvatietoisuuden perustasosta kohdeyrityksessä aukeaisi.

4.1.1 Koko henkilöstölle lähetetty tietoturvallisuuden lähtökysely

Pilottien kanssa suoritetun kyselyn seurauksena päätettiin suorittaa kaikille kohdeyrityksen loppukäyttäjille suunnattu Tietoturvallisuuden lähtökysely. Lähtökyselyn tarkoituksena oli vahvistaa tulevan jalkautuksen ydinalueita, joihin perehdytystavassa tullaan syventymään tarkemmin. Pilotoijilta saatujen kommenttien perusteella päätettiin olla muuttamatta alkuperäistä kyselyä. Muutamia kommentteja kyselystä olivat mm.:

”Kysely asiallinen ja tarpeellinen.”

”Selkeä ja nopea tehdä.”

”Tämä on hyvä!”

”Ihan hyvä peruskäyttäjien tietotason kartoittamiseen.”

”Ihan ok, jos todella tietoa haluaa ihmisten tietämyksen tasosta aihealueella, kysely olisi voinut olla yksityiskohtaisempi. Mutta toisaalta sopivan lyhyt, jotta vastaamisen "viitsi" tehdä :)”

”Hyvä kysely :)”

”Kysely on mielestäni hyvä. IT voisi pitää infotilaisuuksia useammin.”

”Hyvä muistutus tietoturvan tärkeydestä.”

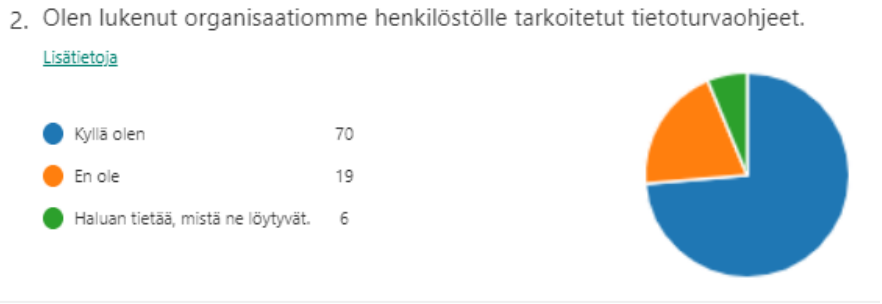
Lopullinen loppukäyttäjille lähetetty kysely tietoturvallisuudesta lähti kaikille 274 käyttäjälle, joista n. 220 henkilöllä on oma työasema. Kysely suoritettiin anonyymisti sähköpostilla, josta löytyi tietoturvallinen linkki itse kyselyyn. Vastausaika oli 11.10-1.11.2019, jona aikana kyselyyn vastasi 92 käyttäjää. Tätä pidetään kohdeyrityksessä riittävänä vastausmääränä. Vastausmäärään vaikuttaa työasemien määrän suhde kyselyn vastaanottajiin sekä vastaajien työnkuva sekä luonnollisesti kuinka merkittäväksi käyttäjä tietoturvan omassa roolissaan kokee.

Kuva 14 esittää otetta kyselyn etusivusta, jolla haettiin kohdeyrityksen yhteisöllisyyttä.

Kuva 14: Tietoturvallisuuskyselyyn etusivu

Ensimmäisen loppukäyttäjille suunnatun kyselyn tarkoitus oli selvittää kohdeyrityksen henkilöstön ymmärrystä yleisistä tietoturva-asioista sekä selvittää, mitkä asiat heille ovat epäselviä tai mikä heitä tietoturva-asioissa mietityttää. Vastausten perusteella määriteltiin kohteet, joihin tiedon jakamisessa pitää jatkossa perehtyä erikseen. Kysymyksistä kuusi ensimmäistä oli pakollisia. Toisaalta osaan kysymyksistä löytyi useampi oikea vastaus. Oikeita vastauksia kyselyssä ei näytetty, vaikka Forms -kyselypohja sen mahdollistaakin.

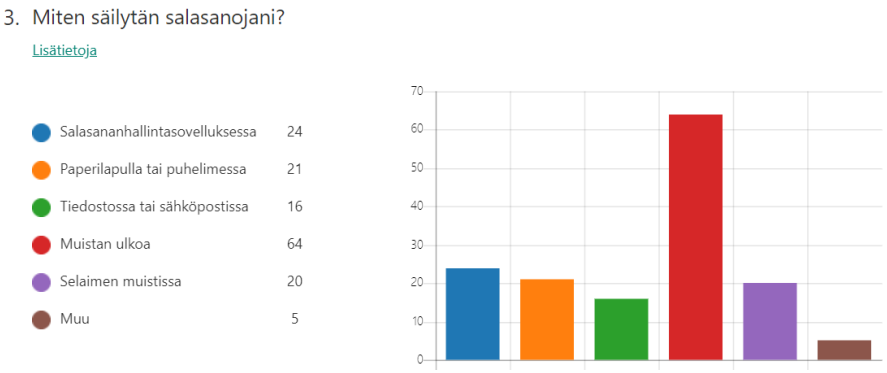
Tulosten analysoinnissa hyödynnettiin sekä luetteloita (esim. vapaat kirjoituskentät) sekä graafisia kuvaajia, kuten piirakka- ja pylväsdiagrammit. Esimerkiksi kysymyksessä kaksi esitettiin kysymys henkilöstön tietoturvaohjeiden lukemiseen liittyen, tästä Kuva 15. Piirakkamainen kaavio antaa selkeän kokonaiskuvan siitä, miten moni on ohjeistukset lukenut (70 vastaajaa) sekä niistä, jotka eivät ole niitä lukeneet (19 vastaajaa). Lisäksi kuusi käyttäjää ei tiedä, mistä ohjeistukset ovat löydettävissä.



Kuva 15: Tietoturvatietoisuus alkukysely, kysymys 2, piirakkadiagrammi

Vastauksista voimme päätellä, että tietoturvaperehdytyksiin ja ohjeistusten sijaintiin tulee kiinnittää huomiota, jolloin sekä tiedotusta, että ohjeiden löytämisen selkeyttä tulee lisätä. Kuitenkin 74 prosenttia vastaajista on tutustunut ohjeisiin.

Toisena esimerkkinä pylväsdiagrammin käytöstä kyselyn vastausten analysoinnissa oli kysymyksessä kolme esitetty kysymys liittyen salasanojen säilytyksen ja muistamisen menetelmiin. Kyseinen esitystapa sopii paremmin kuvaamaan kuuden eri vastausvaihtoehdon jakaumaa. Kuva 16 kuvaa kysymyksen kolme vastauksia pylväskaavion muodossa.



Kuva 16: Tietoturvatietoisuus alkukysely, kysymys 3, pylväsdiagrammi

Koska kohdeyritys toimii monisovellusympäristössä, on salasanoja kymmeniä, jollei osalla henkilöstöstä jopa satoja, sovellusten käyttömäärästä riippuen (Jansson, 2019b). Salasanojen säilytyksessä havaitaan jonkin verran vaihtelua. Yllättävän moni muistaa kaikki salasanat ulkoa, mutta toisaalta syntyy epäilys, käytetäänkö paljon samoja salasanoja eri sovelluksissa, järjestelmissä ja sivustoilla. Suositeltava toimenpide voisi olla salasanan hallintajärjestelmien läpikäynti ja tietohallinnon suositukset niistä henkilöstölle. Myös keskitetty jakelu käyttäjien työasemille voidaan ottaa huomioon, jolloin kaikille työasemia käyttäville työntekijöille mahdollistetaan sama yrityskohtainen järjestelmä.

Tehdyn tietoturvakyselyn perusteella saaduista vastauksista suoritettiin analyysi ja suositeltiin tietoturvaperehdytysten kohteet, joihin tulee kiinnittää erityisesti huomiota. Perehdytystapaan liittyen päätettiin suorittaa toinen pilotointi, jonka perusteella pyrittiin löytämään nimenomaan kohdeyrityksen henkilökunnalle soveltuva perehdytystapa ja näin edistää työn kohteena olevaa tietoturvakulttuurin kehittämistä tältä osin. Loppukäyttäjille suunnattu kysely toi esille muutamia asioita, joihin tulee jatkossa kiinnittää huomiota tietoturvaperehdytyksien sisällössä. Positiivista oli, että

tietoturvapolitiikasta ollaan hyvinkin tietoisia (kysymys yksi). 99 prosenttia kaikista vastaajista eli 91 henkilöä 92 henkilöstä tiesi, että kohdeyrityksellä on tietoturvapolitiikka. Tietoturvaohjeistukseen perehtyminen on kohtuullisen hyvä. 26 prosenttia vastaajista ei ole tutustunut yrityksen tietoturvaohjeistukseen tai ei tiedä, mistä se on löydettävissä. Prosentuaalinen määrä tarkoittaa vastaajista 25 henkilöä. Kokonaisuutena vastaukset tähän kysymykseen saatiin 95 käyttäjältä – osa on vastannut, ettei ole lukenut eikä tiedä missä ohjeet ovat. Kaikkiaan vain kuusi henkilöä ei tiedä, missä ohjeet ovat.

Kysymys kolme koski salasanojen säilytystä. Jopa 75 prosenttia kaikista vastaajista säilytti salasanoja muulla tavoin kuin luotettavan tekniikan takana. 61 prosenttia vastaajista piti salasanoja omassa muistissaan tai paperilla, loput pitivät niitä puhelimessa, jossain tiedostossa, sähköpostissa, selaimen muistissa tai muussa paikassa. Vain 25 prosenttia käytti jotain salasanan hallintasovellusta. Koska yrityksessä on käyttäjän toimenkuvasta riippuen useita kymmeniä sovelluksia, jotka vaativat salasanoja, on huolestuttavaa, että niiden muistaminen on muistin varassa tai muuten saatavilla.

Neljännessä kysymyksessä tiedusteltiin, mitä käyttäjä tekee, mikäli hän saa epäilyttävän sähköpostin. Kysymyksessä oli mahdollista vastata useampi eri vastaus, joista jokainen oli kuitenkin oikea vastaus. Vastauksia saatiin 89 vastaajalta. Vain yksi heistä vastasi lisäksi muista poikkeavan vastauksen, kuten "estän lähettäjän, puhdistan kansion”, mikä sekään ei ole väärä vastaus. Vastausprosentti tähän kysymykseen oli 97 prosenttia kaikista vastaajista. Vastausten perusteella tietohallinnon tiedotus ja opastustoimet ovat onnistuneita, joten niitä on syytä edelleen jatkaa.

Viides kysymys käsitteli tietomurtojen seurauksia. Myös tähän kysymykseen vastausprosentti oli 97 prosenttia eli 89 työntekijää vastasi kysymykseen. Ainoastaan yksi henkilö otti kantaa kotiin kohdistuvaan tietomurtoon. Yrityksen perehdytykset voisivat näin ollen sisältää myös kotia koskevia uhkatekijöitä, kuten esimerkiksi teemalla ”työkoneen käyttö kotikoneena” ja siitä aiheutuvat uhat. Tämän kysymyksen seurauksena julkaistiin yrityksen Teams’in tiedotuskanavalla Kyberturvallisuus-keskuksen Spoofy-sovellus, jonka avulla kodin tietoisuus tietoturvauhista a niiden torjuntamahdollisuuksista voi kasvaa myös perheen lasten kautta.

Kysymyksissä kuusi ja seitsemän vastaajien oli mahdollista kertoa omin sanoin huolenaiheitaan tietoturvaan liittyen sekä antaa palautetta kyselystä. Vastausten perusteella saatiin hahmotettua käyttäjien huolenaiheita. Päällimmäisiksi asioiksi nousivat runsas salasanojen määrä ja niiden säilyttäminen, monisovellusympäristö, henkilökunnan oma ymmärrys ja osaaminen ja siihen liittyvät mahdollisuudet toimia huolimattomasti. Myös työtovereiden ymmärtämättömyys ja valveutumattomuus tietoturvaan liittyvissä asioissa huolestutti. Näistä johtuen koettiin, että informaatiota ei saatu riittävästi ja näin koulutusta toivottiinkin lisää. Samalla pelättiin hakkereita ja erilaisia tietomurtoja liittyen niin työn kuin kodin tietoturvallisuuteen. Kyselyn markkinoinnissa kannustettiin ihmisiä kirjaamaan myös kodin tietoturvallisuuden huolia palautteisiin. Loppukäyttäjien huolien aiheet halutaan esittää varsinaisten tuloskaavioiden lisäksi ns. Word Cloud’in muodossa. Kysymyksestä kuusi muodostettu sanapilvi esitetään alla, Kuva 17. Työkaluna on käytetty https://wordart.com/-sivuston sanapilven muodostusta.

Kuva 17: Tietoturvallisuuden kyselyn WordCloud

Edellä kuvatussa ensimmäisessä vaiheessa suoritetun tietoturvan ymmärryksen nykykuvaa selvittävän kyselyn tarkoituksena oli kartoittaa kohdeyrityksen henkilökunnan tietoturvaosaamisen ja sen ymmärryksen tasoa. Kyselyn avulla saatiin myös tietoa siitä, millaista perehdytystä yrityksessä jatkossa tarvitaan.

4.2 Tietoturvan jalkautusmenetelmän etsiminen uusien pilottien avustuksella

Aiempana on kuvattu kappaleessa 2.4 mekanismeja, miten ihminen oppii parhaiten. Näihin pohjautuen työssä päätettiin edetä mikro-oppimisen mallia soveltaen, mutta hyödyntäen jollain tavoin digitaalista oppimisalustaa. Tiedon jalkauttamisen mekanismia haluttiin etsiä vielä toisen pilotoinnin avulla. Tähän pilotointiin haettiin osittain mallia ammattikorkeakoulujen ja yliopistojen opetusmetodeista, mutta myös perinteisiä menetelmiä haluttiin käyttää. Kohdeyrityksen LABS-menetelmä toimi selvittämisessä apuna.

Aiemmin kuvatun Tietoturvallisuuden lähtökyselyn seurauksena päätettiin lähteä selvittämään, mikä on paras lähestymistapa kohdeyrityksen henkilöstön perehdyttämisessä. Tähän mennessä oli saatu tietoa siitä, mitkä asiat tuli erityisesti ottaa huomioon perehdytyksessä. Seuraavassa vaiheessa haettiin nimenomaan itsenäistä perehtymistä tukevaa jalkautustapaa. Kirjallisuudesta sekä muiden energiayhtiöiden kokemusten perusteella, tarjolla on muutama hyvä tapa lähestyä loppukäyttäjiä. Vahvimpana ajatuksena oli löytää tapa, joka tuo asiaa sopivissa kokonaisuuksissa, helposti ymmärrettävänä, jopa omaan työympäristöön verrattavissa olevasti sekä tarinallisesti kerrottuna. Ensimmäisenä tavoitteena oli kartoittaa erityyppisten lähestymistapojen kautta, mikä perehdytystapa olisi soveltuvin kyseisessä tapauksessa. Alustavasti ajateltiin, että vastaavaa perehdytystapaa voidaan käyttää myös toisenlaisessa aiheessa, kuten esimerkiksi työmaakoulutuksissa.

Lähestymistavan selvittämiseksi valittiin heterogeeninen, mutta tiedossa oleva, otos henkilöstöä. Pilottiryhmän kooksi valittiin lopulta noin 20 henkilöä, joiden avulla tapoja haettiin. Pilotit koostuivat johtajista, toimihenkilöistä ja työntekijöistä, jotka työskentelevät toimistossa, maastossa sekä voimalaitoksissa. Pilotoinnin jälkeen analysoitiin tulokset sekä päätettiin tapa, jolla tietoturvaa tullaan perehdyttämään ja kouluttamaan koko

henkilöstöä miellyttävällä tavalla. Koska valittu ryhmä oli varsin heterogeeninen, päädyttiin opetustapojen valinta tekemään kohdeyrityksessä käytössä olevan ns. LABS –kyselyn avulla. LABS-kysely voidaan muodostaa eri ryhmille sekä eri tarkoituksiin joka kerta eri tavoin (Niemi, 2020). Kohdeyritys on hakenut vastaavilla kyselyillä mm. asiakkaiden mieltymyksiä sekä oman henkilöstön kiinnostuksen kohteita vapaa-aikatoimintaan.

Tietoturvan perehdytystavan LABS päätettiin jakaa neljään osa-alueeseen. Tarkoitus oli esittää pilottiryhmän eri jäsenille erilaisia perehdytysmenetelmiä ja vastausten perusteella selvittää, mikä tai mitkä näistä tavoista saavat parhaat vastaukset. Jokaisen toteutuksen jälkeen suoritettiin sama loppukysely kohdehenkilöltä oppimistyylin tulosten selvittämiseksi. Loppukysely puolestaan tehtiin hyväksikäyttäen ensimmäisen kyselyn tapaan O365-perheen Forms-kyselylomaketta. Perehdytyksen pilotoinnissa esitetty loppukysely toimitettiin kaikille perehdytysvaiheen pilotoijille. Perehdytysten sisällön tuli säilyä pilotoinnissa saman kuin kohdeyrityksessä jo käytössä oleva perehdytysaineiston oli. Näin haluttiin turvata LABS-kyselyn tasa-arvoisuus toisiinsa verrattuna. Perehdytysaineiston asioita on läpikäyty aiemmin kohdeyrityksessä ryhmissä, yksityisesti sekä tiedotusluoteisesti, joten henkilökunnalla piti olla sama tieto olemassa.

Ensimmäinen tapa pohjautui ryhmäkohtaiseen läpikäyntiin, jossa materiaalina toimi olemassa oleva Perehdytys tietoturvaan -esitysmateriaali (Jansson, 2019c). Kyseinen materiaali läpikäytiin valikoituneen kohderyhmän kanssa kahdessa osassa henkilökohtaisesti ICT-palvelupäällikön toimesta, koska perehdytystapa edellyttää kouluttajan läsnäoloa materiaalin kerronnallisen osan vuoksi. Materiaali sisältää tarinoita sekä niiden tukena napakoita, ranskalaisin viivoin merkattuja kommentteja. Itsenäinen opiskelu on todennäköisesti hieman vaikeaa materiaalista johtuen. Kyseinen perehdytystapa on aikaa vievä ja vaatii materiaalin tekijän kertomukset, jotta sen sisäistäminen helpottuu. Tässä ensimmäisessä tavassa tietoturvallisuuden loppukysely toimitettiin osallistujille kahden viikon päästä perehdytyksestä.

Pilotoinnin toisessa ryhmässä haluttiin pilotteja lähestyä materiaalilla, jossa oli yhdistetty alkuperäisen materiaalin tärkeimmiksi nähdyt tietoturvallisuuden aiheet sekä saatu mukaan niihin liittyviä tarinoita videoiden muodossa. Videomateriaalit hankittiin 2NS - Second Nature Securityn avustuksella. Lisäideoina ajateltiin myös omia videointeja tarinoista, joita perehdytysmateriaalissa jo läpikäydään henkilökohtaisissa läpikäynneissä, mutta videointimateriaalin tekoa ei nyt nähty kohdeyrityksen ydinbisnekseksi. Ajatus kuitenkin otettiin huomioon jatkoa ajatellen sekä materiaalin muokkauksia ajatellen. Tämä perehdytystapa oli kohtuullisen työläs toteuttaa siihen valituilla välineillä niiden vaatiman opiskelun vuoksi. Perehdytysmateriaali koostui O365-perheen Stream- ja Forms -työkalujen yhdistelmänä, jolloin sekä asiasivuja, että videoita voitiin upottaa materiaaleihin. Perehdytysmateriaaleista päätettiin tehdä muutamia lyhyitä, n. 3-4 minuutin mittaisia tietoiskuja, jolloin käyttäjällä on mahdollisuus läpikäydä ne oman ajan puitteissa. Tietoturvalle perustettiin oma Stream -kanava henkilökunnan seurattavaksi. Materiaalia voidaan muokata ja täydentää Forms-lomakkeiden osalta, jotta tarinat kehittyvät ja pysyvät ajan hengessä mukana. Myös videomateriaalia voidaan hankkia halutessa lisää.

Kolmantena perehdytyskulttuuria testaavana menetelmän haluttiin käyttää ns. Flipped classroom -tekniikkaa. Tämän tekniikan kautta työntekijöille lähetetään ensin toisen vaiheen kaltainen perehdytysmateriaali, jossa yhdistyvät videot ja asia. Tämän lisäksi

olemassa oleva materiaali läpikäydään vielä läpi yhdessä kouluttajan kanssa (Venhe, 2018). Tässä tavassa haluttiin läpikäydä lähiperehdytys olemassa olevan materiaalin kautta. Näin mahdollistettiin erilaisten esimerkkien ja tarinoiden käyttö materiaalissa. Periaatteessa kolmas menetelmä yhdistää ensimmäisen ja toisen perehdytystavan. Loppukysely tehtiin molempien läpikäyntien jälkeen. Tämä perehdytystapa edellyttää kohdeyrityksen henkilökunnalta etukäteisperehtymistä tavan kaksi aineiston pohjalta. Sen lisäksi materiaali läpikäydään uudelleen syvemmin, kouluttajan muodostamien tarinoiden kautta ja kohderyhmässä keskustellen.

Neljäs LABS -kyselyn kautta suoritettu perehdytystapa ei vaadi erikseen varsinaista perehdytystä, vaan oppiminen perustuu saatuihin tiedotteisiin sekä aiempiin perehdytyksiin. Tähän pilotointitapaan valitut henkilöt saivat ainoastaan suoran loppukyselyn, johon heidän tuli vastata.

Edellä mainittujen neljän erilaisen perehdytysmekanismin perusteella tehdyn LABS-kyselyn perusteella oli tarkoitus löytää kohderyhmälle ja yritykselle paras tapa oppia ja sisäistää asioita. Uuden tavan löytyminen merkitsee samalla perehdytyskulttuurin muuttumista kohdeyrityksessä. Seuraavassa läpikäydään vielä kyselyä, joka kaikkien LABS-mekanismiin osallistuneiden pilottien tuli täyttää edellä mainittujen neljän perehdytyksen jälkeen. LABS -mekanismin avulla suoritettujen koulutusten lopuksi tehtiin pilottiryhmille lopputentti. Tentti koostui samoista aihealueista kuin alkuperäinen tietoturvan perehdytysmateriaali, sisältäen kuitenkin myös asioita, jotka esitettiin LABS-kyselyn vaiheissa kaksi ja kolme. Loppukysely tehtiin käyttäen O365-sovellusperheen Forms -lomaketta, jonne liitettiin alkuperäisen materiaalin kuvia sekä 2NS - Second Nature Security -yrityksen kysymyspatteristo niiltä osin, jotka liittyivät kohdeyrityksen alkuperäiseen tietoturvan perehdytysaineistoon. Kysymyksiin liitettiin vastauksia niin 2NS:n aineistosta kuin kohdeyrityksen ohjeistuksista. Vastaajan vastaukset pisteytettiin ja vastausten jälkeen henkilö sai tulokset sähköisesti. Oikeat vastaukset näkyivät vastaus -osiossa, jolloin henkilön oli mahdollista kyselyn lopuksi myös oppia. Tehdyn kyselyn tarkoituksena oli nimenomaan löytää se tapa neljästä LABS-menetelmästä, joka soveltuu parhaiten kohderyhmille. Tulosten perusteella voitiin nostaa yksi tapa tavoitelluksi menetelmäksi. Kuva 18 esittelee viimeisen lopputentin alustustekstiä, jossa pohjustettiin tämän kyselyn tarkoitusta ja sen käyttökohdetta.

Tietoturvakysely

Sinut on valittu pilottiryhmään, joiden vastausten perusteella pyritään löytämään Pori Energialle meille soveltuva perehdytyskulttuuri. Kysely liittyy tekemääni diplomityöhön.
Tätä kulttuuria haetaan ensisijaisesti tietoturvaperehdytyksen kautta. Tietoturvakyselyn tarkoituksena on saada tietoa siitä, miten hyvin yrityksemme henkilökunta hallitsee aiemmin saadun tiedon perusteella yrityksellemme tärkeät tietoturvaan liittyvät asiat.

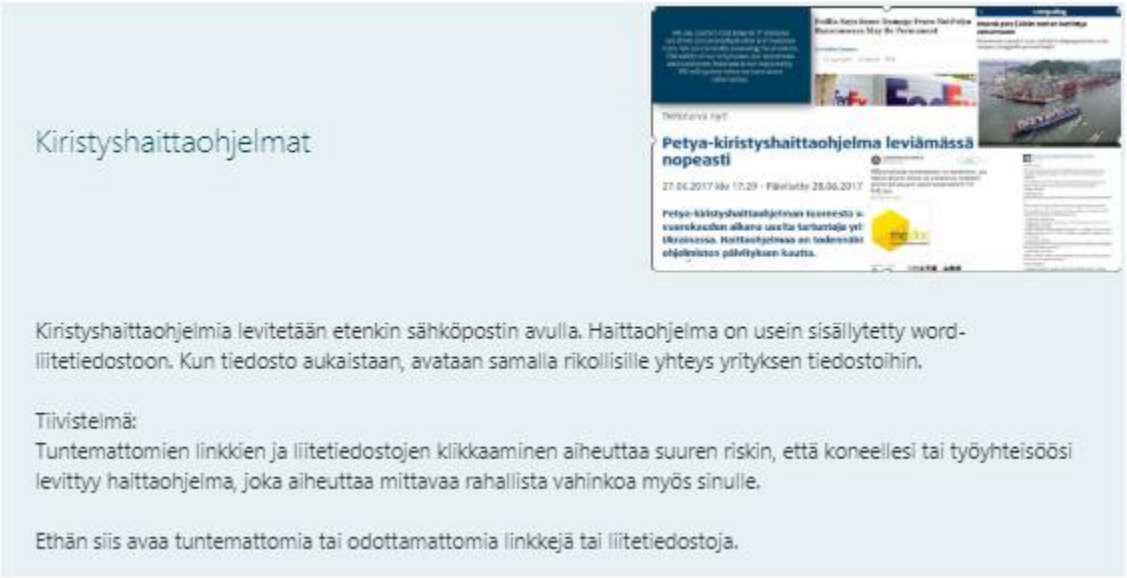
Olen valinnut mukaan heterogeenisen ryhmän vastaanottajia, joiden perehdytysmekanismit voidaan jakaa varsinaisesti neljään ryhmään:
1. Henkilöt, jotka ovat osallistuneet perinteiseen ryhmätilaisuuteen Pori Energian nykyistä aineistoa läpikäyden
2. Henkilöt, jotka ovat saaneet aiheeseen liittyvän visuaalisen ja kirjallisen aineiston (toteutus videot ja tekstit) itsenäiseen tarkasteluun hänelle sopivaan aikaan annetun aikarajan puitteissa.
3. Henkilöt, jotka ovat saaneet aiheeseen liittyvän visuaalisen ja kirjallisen aineiston (toteutus videot ja tekstit) ja joiden kanssa sen lisäksi on läpikäyty asia perinteisellä ryhmätilaisuudella (Flipped classroom -menetelmä)
4. Henkilöt, jotka ovat lukeneet yleisiä tiedotteita ja M-filesin materiaaleja omatoimisesti

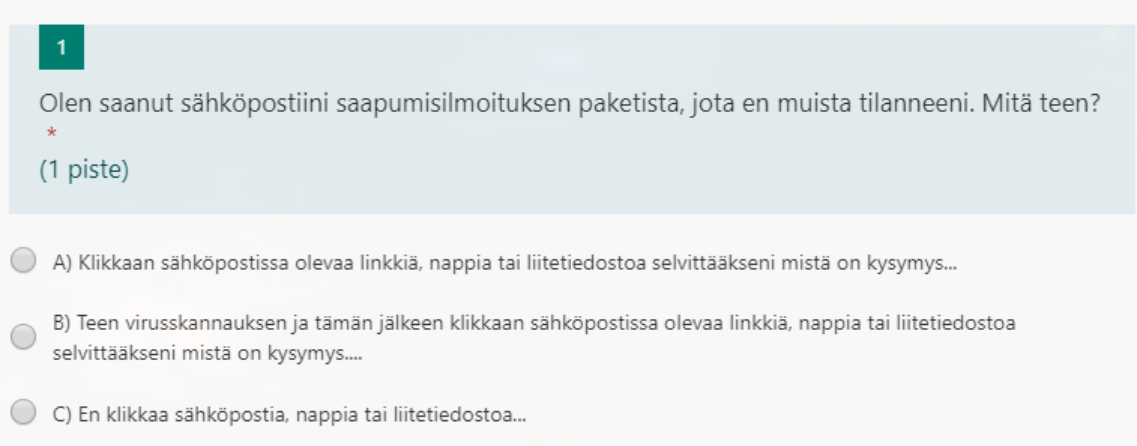
Kysely tehdään anonyymisti ja vastauksia tarkastelee ainoastaan Pori Energian Tietohallinto. Tuloksien läpikäynti ja lopputulema kirjataan valmisteilla olevaan diplomityöhön.

Kiitos yhteistyöstäsi, vastaathan kyselyyn 20.3.2020 mennessä.

Kuva 18: Piloteille tarkoitettu tietoturvaperehdytyksen loppukysely

Kuva 19 näyttää esimerkkiä kysymyksestä, jollaisiin käyttäjien tuli vastata. Kyselyn alueet oli jaettu kokonaisuuksiin, jolloin käyttäjän oli helppo yhdistää asiat aiemmin oppimaansa tietoon. Kuvien tarkoituksena oli muistuttaa perehdytysten kertomuksista.





Kuva 19: Ote piloteille esitetystä kyselystä

Kyselyn perusteella lähdettiin seuraavassa vaiheessa tuottamaan tulosten mukaista aineistoa koko henkilöstölle.

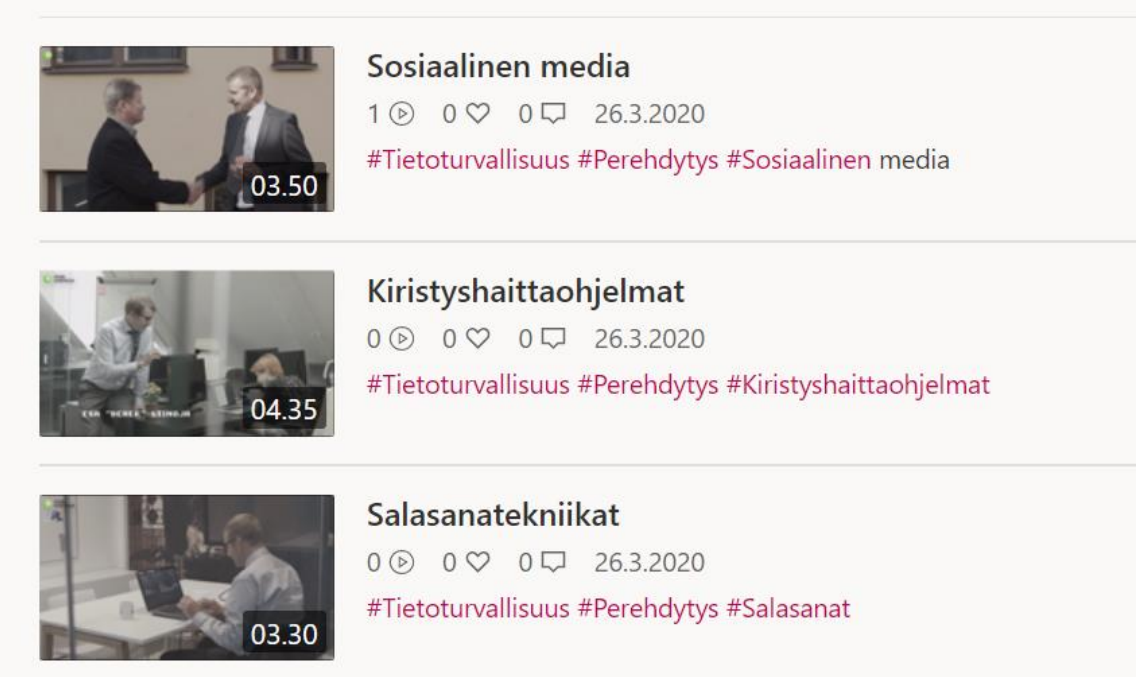
4.2.1 Opetustyylin uuden pilotoinnin tulokset ja perehdytysmenetelmän valinta henkilöstölle

Pilottivaihe toteutettiin maaliskuussa 2020. Jotta oikea perehdytystapa tulisi valittua, suoritettiin pilottien lopputentin kautta arviointi tavasta, jolla kohdehenkilöt sisäistivät asiat parhaiten. Kyseinen tapa valittiin jatkoa varten mukaan uuden perehdytyskulttuurin kehittämiseen osana kehityksen ensimmäistä vaihetta. Tästä johtuen valittiin uusi opetustyyli, jota päätettiin lähteä jalkauttamaan koko henkilökunnalle. Henkilökunnan

kokonaismäärä tuolloin oli 273 henkeä, joista 19 oli määräaikaisia. Mukana ovat tytäryhtiön sekä osaomisteisen (49%) yrityksen henkilöstö.

Perehdytystavan pilotointivaiheen perusteella päädyttiin valitsemaan tietoturvan perehdytystavaksi yhdistelmä videoinnista ja teksteistä eli tapa kaksi. Tapa kolme eli ns. Flipped classroom -tekniikka vaikutti myös lupaavalta, mutta sitoisi nykyisen perehdytystavan kaltaisesti yhteistä aikaa niin perehdyttäjän kuin perehdytettävän kalentereista. Näin ollen tapa kolme ei ole täysin itsenäinen, mutta mahdollistaa epäselvien asioiden läpikäynnin sekä kysymykset luontevasti. Videomateriaalin luonnissa hyödynnettiin 2NS - Second Nature Securityn aineistoja muokaten niistä mikro-oppimiseen soveltuva koulutusmateriaali. Luontivaiheessa pyrittiin käyttämään loogista etenemistapaa. Perehdytysmateriaali mikro-oppimisessa mukailee olemassa olevaa materiaalia, joskin siitä nostettiin esille merkityksellisimmät asiat, jotta itse oppimissisältö ei kasvanut liian suureksi ja sitä kautta liian vaikeaselkoiseksi. Oppimissisältö pyrittiin pitämään kansankielisenä ja selkeänä. Hyödyntämällä 2NS:n materiaalissa olevia videoita, saatiin materiaaliin mukaan oikeita esimerkkejä asioista, joita kohtaamme lähes joka päivä tietoturvan suhteen. Koulutettavan rooli helpottuu, kun asioita yhdistetään oikeaan ja ihmistä lähellä olevaan tekemiseen. Second Nature Securityn, 2NS, kautta hankittu materiaali sekä omista aiemmista materiaaleista poimittu data yhdistettiin ja päädyttiin luomaan kohdeyritykselle O365-perheen Stream'in Tietoturvallisuus -kanava. Kanava sisältää tietoturvallisuuden aihealueita, joiden kesto on n.4-5 minuuttia ja joita henkilöstö voi läpikäydä oman ajankäyttönsä puitteissa yrityksen tietoturvan vuosikelloon asettamissa aikaikkunoissa. Seurantaa ajatellen, Stream ei sisällä tietoa katsojista. Katsomiskerrat kuitenkin rekisteröidään määrällisesti. Mikäli halutaan seurata sitä tietoa, ketkä kyseiset perehdytykset ovat läpikäyneet, tulee materiaalit tehdä toisin ja viedä ne Forms -lomakkeiden kautta toteutukseen.

Perehdytysmateriaalin ensimmäinen osa jaetaan sähköisesti koko henkilöstölle huhti-toukokuun 2020 aikana. Tätä toimenpidettä ennen, esimiesorganisaatiota muistutetaan materiaalin läpikäynnistä mm. tiimipalavereissa, jolloin ajankäyttö voidaan maksimoida. Osana esimiesten tehtäviä on kannustaa uuden tietoturvallisuuden perehdytysmateriaalin läpikäyntiin, jotta itse tietoturvakulttuuri saa mahdollisuuden kehittyä. Osana toteutettavia Stream -kanavan koulutuksia, toteutetaan Teams -kanavalla jatkuvaa tiedotusta tietoturvaan liittyvistä asioista, Kybersäästä sekä mm. kausiluonteisista tunkeutumisyrityksistä. Stream'iin on luotu oma kanava tietoturvaperehdytyksille. Ohessa Kuva 20 on ensimmäisen perehdytysosan Tietoturva-kanavan Osa 1. Kohdeyrityksen pääkanavan alle luotava Tietoturva -kanava sisältää tietoturvaperehdytyksen osa-alueet, jotka mukailevat vuosikellon koulutusohjelmaa. Lisäksi se sisältää kesätyöntekijöille ja muille harjoittelijoille suunnatun osuuden.



Kuva 20: Tietoturvan Stream-kanava, Tietoturvaperehdytyksen osa 1

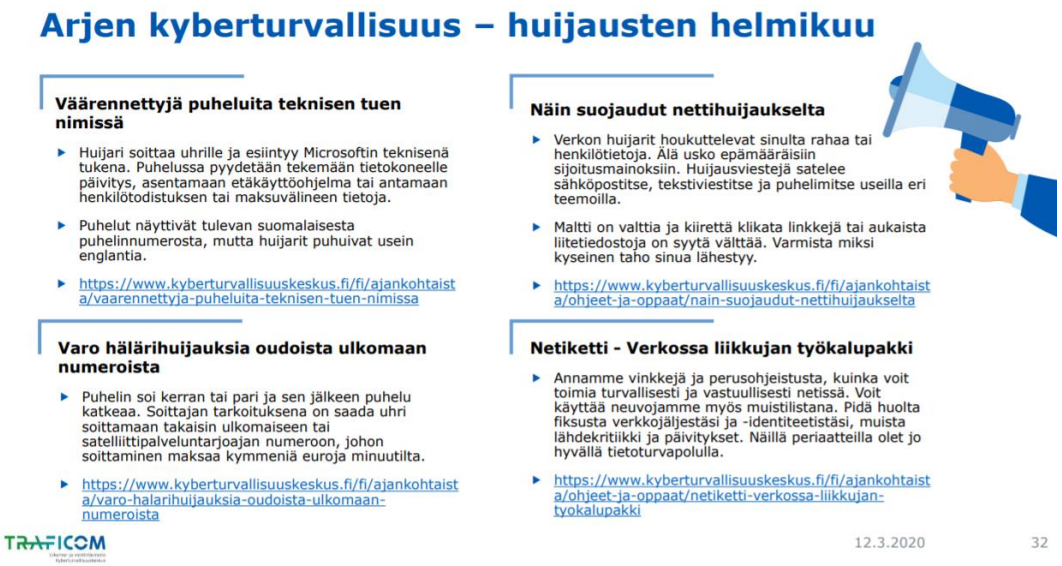
Edellä oleva videokirjasto mukailee vuosikellossa kuvattua perehdytyksen osaa yksi, joka ajallisesti olisi normaalissa aikataulussa vuoden alkupuolella.

4.2.2 Kybersää osana tietoturvakulttuuria

Osana kulttuuria on kohdeyrityksessä päätetty ottaa käyttöön Kyberturvallisuuskeskuksen Kybersään säännöllinen seuraaminen. Tällä tavoin henkilöstöllä on mahdollisuus tutustua lähes reaaliaikaiseen kyberuhkatilanteeseen. Kyberturvallisuuskeskuksen tarjoama palvelu antaa kuvan kuluvan kuukauden aikana tapahtuneista tietoturvan poikkeamista sekä uusista tietoturvailmiöistä. Traficomin tarjoama palvelu tarkastelee useampaa kokonaisuutta, joihin mm. kuuluvat tietoturvan kehitys ja siihen kuuluvat lakiasiat, haittaohjelmat ja tietojärjestelmien sekä -sovellusten haavoittuvuudet, kalasteluviestit sekä huijaukset. Kybersää perehtyy myös esineiden internetin eli IoT:n tietoturvaa, jolloin se palvelee myös kotikäyttäjiä. Kaiken kaikkiaan kybersää koostuu seitsemästä erilaisesta osa-alueesta, joista edellä lueteltiin vain osa niistä. (Traficom, 2020) Kohdeyrityksessä kybersään esittäminen on toteutettu osana Info-TV:n ohjelmaa ja päivittyy kuukausittain kaikkien nähtäville. Alla on näkymä helmikuun 2020 suurimmista uhkatekijöistä, Kuva 21.

Kuva 21: Kybersään tilanne helmikuussa 2020 (Traficom, 2020)

Paitsi tiedotusta, kybersää kertoo myös tilanteista, joita ihmiset kohtaavat päivittäin sekä ohjeistaa toimimaan oikein. Tästä esimerkkinä Kuva 22, joka on ajanjaksollisesti helmikuulta 2020.



Kuva 22: Arjen kyberturvallisuus - Kybersää (Traficom, 2020)

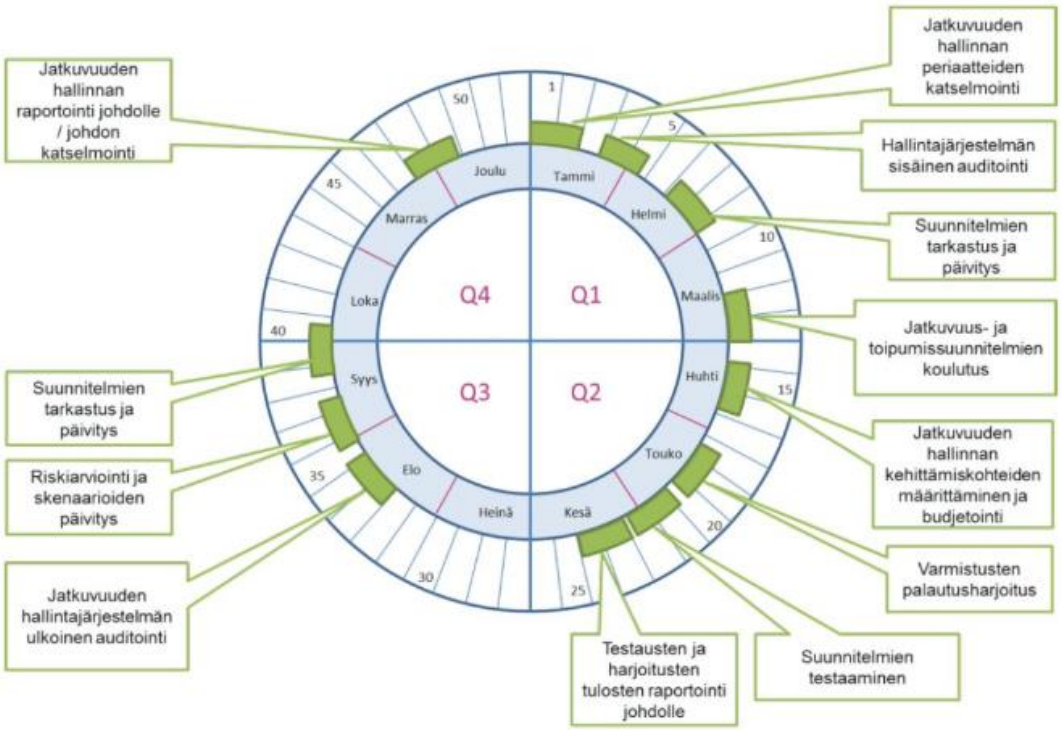
Kybersää kertoo samalla Top 5-listan kyberuhista, jolloin lukija saa yhdellä silmäyksellä käsityksen niistä seikoista, joihin pitää erityisesti kiinnittää huomiota tietoturvallisen toiminnan edistämiseksi. Vaikka kybersää on tarkoitettu ensisijaisesti tietoturvasta vastaaville henkilöille, on suositeltavaa, että tietoa jaetaan avoimesti kohdeyrityksessä. Kulttuuria ollaankin jatkuvasti kehittämässä avoimempaan suuntaan, jotta tietoa saadaan mahdollisimman nopeasti, sitä jaetaan nopeasti kohdeyrityksessä käytössä olevilla viestinnän kanavilla, kuten Teams, kirjalliset viikkotiedotteet, sähköposti sekä Info-TV. Kohdeyritys rohkaisee jatkuvasti henkilökuntaansa jakamaan tietoa, kysymään lisää ja neuvomaan kollegoitaan avoimesti. Viimeisen vuoden aikana tämä

kulttuurimuutos on näkynyt kaikkien arkipäivässä. Keskustelu asioista käy vilkkaana Teams'in kautta, johtajien näyttäessä omaa esimerkkiään tässä toiminnassa.

Kohdeyrityksen tietoturvakulttuuriin halutaan tuoda mukaan perehdytysten jatkuvuus. Tästä syystä yritykselle suunniteltiin ympäri vuoden pyörivä koulutusaineisto, jossa samalla painotetaan esimerkiksi kesäaikana sähköpostitse tulevien uhkien taajuutta ja muistutetaan erilaisista uhkatekijöistä henkilökuntaa. Lisäksi mukaan perehdytyksiin otettiin kesätyöntekijöiden oma ohjelma, jossa läpikäydään erillinen perehdytyspaketti esimiehen avustuksella, Näistä rakennettiin yritykselle tietoturvaperehdytysten vuosikello, joka myöhemmin synkronoidaan tietohallinnon vuosikelloon osana vuoden mittaan tapahtuvia toimia.

4.3 Tietohallinnon vuosikello

Vuosikellon merkitys voi olla yritykselle hyvin merkittävä. Vuosikellon avulla voidaan kuvata tai hahmotella yrityksen koko vuoden tärkeimpiä tehtäviä, se voi koskea kerralla koko organisaatiota tai vain jotain tiettyä osaa tai osastoa. Vuosikello on visuaalinen tapa näyttää vuoteen kuuluvat teemat sekä tehtävät ja samalla esimerkiksi osaston toimintoihin voidaan liittää koko kohdeyritystä koskevia tehtäviä, kuten budjetointi (Plandisc, 2020). Vuosikellon pohjalta suunnitelmia voidaan tarkentaa ja tehdä niistä yksityiskohtaisempi suunnitelma viikkotasolle asti (Digimoguli Oy, 2019). Jotta tietoturva tulisi osaksi Tietohallinnon muita toimintoja, päätettiin tehdä tietoturvakoulutusten vuosikello -suunnitelma. Suunnitelmassa käytetään hyväksi 2NS:n materiaaleja ja niihin liittyviä käyttösuosituksia. Vuosikellon pohjalta tietohallinto tarjoaa hyvän kokonaiskuvan koulutussykleistään. Tämä omalta osaltaan luo uutta tietoturvan perehdytyskulttuuria.



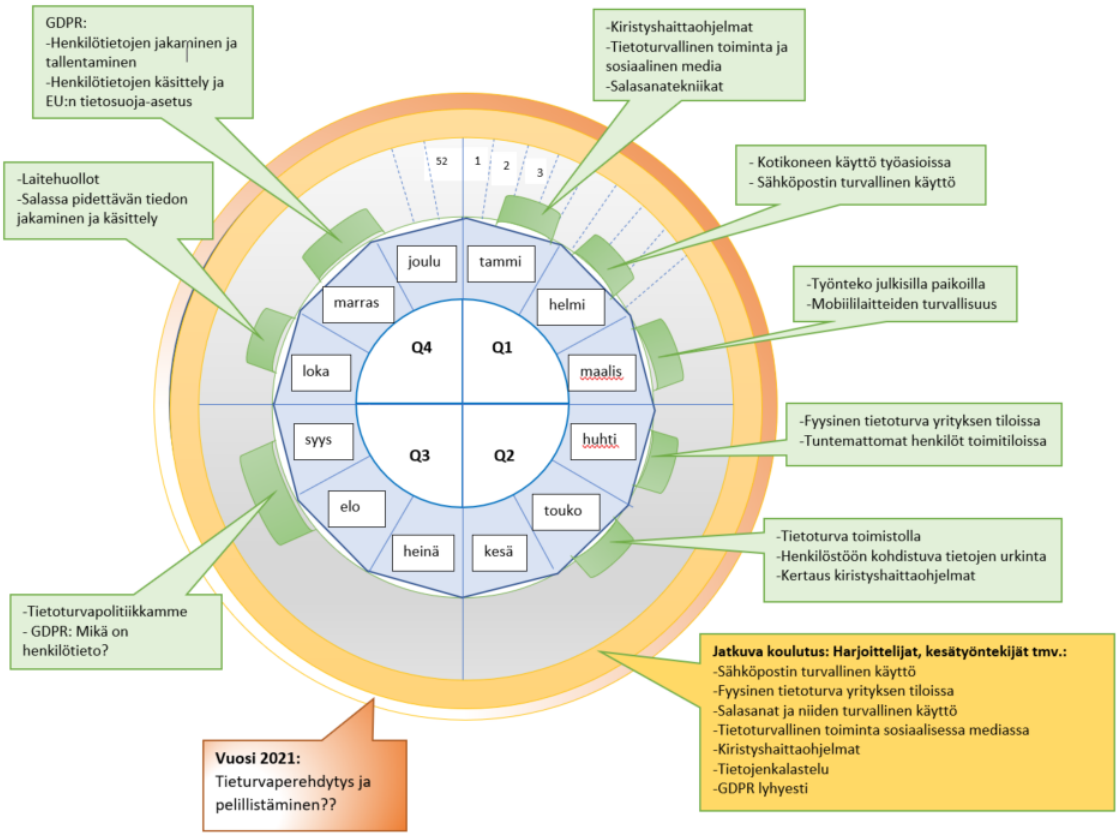
Kuva 23: Valtiovarainministeriön esimerkki vuosikellosta, VAHTI 2/2016 Liite 1 (Valtiovarainministeriö, 2016)

Vuosikello toimii kuten varsinainen kello, mutta aikamääreet ovat kuukausia, viikkoja ja päiviä, tarkkuudesta riippuen. Vuosikello onkin havainnollinen väline myös viestintään. Sen avulla voi myös ennakoida tehtäviä, liittää tekemiset prosesseihin ja se kertoo mahdollisista töiden päällekkäisyyksistä. Organisaation vuosikellot, ainakin osaston sisällä, kannattaa kytkeä toisiinsa, jotta koko osaston työt voidaan kellottaa suhteessa toisiinsa liiallisen työruuhkauman välttämiseksi. Yllä olevassa kuvassa, Kuva 23, on esitetty yksi esimerkki vuosikellosta, jota Valtionvarainministeriö käyttää esimerkkinä jatkuvuuden hallintaan. Vastaavaa vuosikelloa voidaan hyödyntää kohdeyrityksen tietohallinnon ja tietoturvan koulutusten kuvaamisessa.

Vuosikellon suunnittelussa huomioitiin vuodenajan ympärille asettuvat työajat sekä osittain mukaan otettiin erityisesti kesää ennen alkavat kalasteluviestit ja niistä muistuttaminen. Valitut osa-alueet vievät käyttäjältä aikaa kukin n.4 minuuttia, joten pisin kokonaisuus syntyy yli 2kk:n työsuhteen omaaville harjoittelijoille ja kesätyöntekijöille, joiden tulee työsuhteensa aikana läpikäydä seitsemän eri jaksoa. Lyhyemmät työsuhteet voidaan rakentaa erikseen riippuen työtehtävistä.

Pelillistämisestä tulee eittämättä yksi perehdytyskulttuurin aluevaltaus kohdeyrityksessä. Se mahdollistaa ihmisiä motivoivamman tavan oppia uusia ja vanhojakin asioita sekä samalla se mahdollistaa esimerkiksi osastojen välisen tietokilpailun. Tämän toiminnallisuuden toteuttamiseksi tarvitaan kuitenkin alan yhteistyökumppaneita ja aikaa.

Seuraavassa kuvassa, Kuva 24, on esitetty karkealla tasolla kohdeyrityksen vuosille 2020 ja 2021 ajateltu perehdytyskierros. Kuvassa on jo esitetty ajatus pelillistämisen mukaantulosta perehdytyskulttuuriin vuonna 2021.



Kuva 24: Kohdeyrityksen tietoturvaperehdytyksen vuosikello vuosille 2020-2021.

Lopullisen vuosikellon ja siihen sisältyvän koulutusaineiston tuotos tarkentuu kohdeyrityksen ICT-palvelupäällikön kanssa yhteistyössä. Muutoksia perehdytysaikatauluun tulee varmasti, koska tietoturvaa uhkaavat asiat ja sitä suojaavat toimenpiteet muuttuvat kiivaasti. Perehdytysaineistoa tulee päivittää jatkuvasti ja varsin kevyillä muutoksilla, jotta sen luonti ja ylläpito ei olisi liian raskasta.

5. PÄÄTELMÄT

Työn tavoitteena oli kehittää kohdeyritykselle tietoturvakulttuuri. Tätä aihetta lähestytään tässä työssä tietoturvan perehdytystavan eli jalkautuksen etsimisellä, joka puolestaan kehittää tietoturvakulttuuria. Tietoturvan jalkautus lähtee nykyajan tarpeista, kiireestä, projekteista, ihmisten motivaatioon liittyvästä kannustuksesta ja uusien työvälineiden käytöstä. Perinteinen luentomainen perehdytys tai pelkästään kirjallinen materiaali ei 2020 -luvulla enää riitä täyttämään ihmisen mielenkiintoa tai tuo motivaatiota. Pitkien materiaalien lukemiseen ei ole aikaa tai jaksamista, joten perehdytykseen piti saada uudenlaista mielenkiintoa.

Menetelmien pohjatiedoksi työssä läpikäytiin niitä asioita, jotka kohdeyritykselle eli energiayhtiölle ovat merkityksellisiä lainsäätäjän puolesta, lakisisältöä on esitelty liitteessä, LIITE A. Työssä otettiin huomioon alaan liittyvät suositukset ja parhaat toimintatavat, kuten Valtiovarainministeriön tietoturvallisuusohjeistukset eli VAHTI-ohjeistukset (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013). Samalla kuvattiin kriittisen toimialan tärkeimpiä ohjeistuksia koskien tietoturvallista toimintaa ja sitä kautta yrityksen toimintavarmuutta. Työn lopputulemana oli tuottaa hyvin käytännönläheinen työntekijöiden perehdytystapa sekä ottaa kantaa niihin mekanismeihin, joilla ihmisen oppimishaluun voidaan jotenkin vaikuttaa. Vaikuttamisen välineisiin tässä työssä luetaan motivaatio (Huhtanen, 2017), kokemukset perehdytyksen tarpeellisuudesta, ajankäytön järkevöittäminen sekä kokonaisuuksien pilkkomisen vaikutus (Leino, 2019a). Myös perehdytyksen hauskuus ja rentous vaikuttivat perehdytyskulttuurin rakentamiseen.

Kirjallisuutta ja tutkimuksia lukiessani sain havaita, miten eri vuosikymmenien aikana ymmärrys ihmisen oppimistavoista ja vahvuuksista on muuttunut. Oppimiseen vaikuttavia asioita ovat muistin käyttö, motivaatio oppia sekä ihmisen tarkkaavaisuus (Huhtanen, 2017) toisin kuin aiemmin ajateltiin sen olevan lähinnä visuaalista, auditiivista tai kinesteettistä (Tuomola, Maijanen and Prashnig, 1999b). Oppiminen on parhaimmillaan jatkuvaa ja jatkuvasti kehittyvää (Järvilehto and Leino, 2019). Myös tietoturvallisuus on jatkuvaa oppimista ja kehittymistä. Sama pätee niin rikollisiin kuin sen turvaajiin ja menetelmiin. Enää ei ole kysymys pelkästään siitä, että pankkikortin numeroyhdistelmä varastetaan tai yrityksen postia anastetaan. Ollaan huomattavasti syvemmällä ja lähempänä yrityksen työntekijöitä. Työntekijät kohtaavat joka päivä tietoteknisiä uhkia työssään. Tietoturvakulttuuri on henkilön valveutuneisuutta tietoturva-asioissa, tiedon jakoa, onnistuneita perehdytyksiä ja kaiken pohjalla teknisiä toimia, jotka turvaavat tekijöiden selustaa. Ihminen on tietoturvallisuuden heikoin lenkki (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2013). Tästä huolimatta kaiken tiedon tulisi säilyä eheänä, olla saatavilla ja olla luottamuksellista (Pori Energia Oy Johtoryhmä, 2019). Ihmisen tekemät, usein tiedostamattomat, virheet ulkoisten uhkien edessä voivat tuottaa yritykselle todellisen riskin ja sitä kautta vaarantaa sekä yrityksen, että sen asiakkaiden toiminnan. Näistä syistä johtuen kohdeyritys on päättänyt kehittää tietoturvaa yrityksessä niin tekniikan kuin erityisesti loppukäyttäjiensä kautta.

5.1 Johtopäätökset tietoturvakulttuurin kehittymiseen liittyvistä perehdytysmenetelmistä

Tietoturvakulttuurin ja perehdyttämisen välineiden selvittämisessä tuli ensin selvittää millaista aineistoa kohdeyrityksellä oli olemassa ja miten sitä hyödynnettiin. Aineiston todettiin olevan tietynlainen esitysmuotoinen materiaali, jonka tukena kohdeyrityksellä oli tietoturvapolitiikka, tietoturvan pikaohjeet sekä ICT-johtoryhmän kuukausittaiset palaverit aineistoineen. Lisäksi yrityksen toimintajärjestelmästä löytyy useita sisäisiä ohjeita, jotka liittyvät GDPR-tapausten käsittelyyn sekä ohjeistuksiin tietoturvaloukkauksia kohdatessa. Varsinaista loppukäyttäjän perehdytyskulttuuria ei säännöllisessä toteutusmuodossa ollut olemassa. Yrityksellä on uuden henkilön perehdytyssuunnitelma, jossa tietoturvan osuus pyrkii jäämään esimiehen harkinnan varaiseksi asiaksi (Henkilöstöhallinto, 2020).

Menetelmiä mietittäessä lähdettiin liikkeelle siitä, millaisia välineitä kohdeyrityksessä on olemassa. Kohdeyrityksen käyttöön oli hiljattain otettu O365-perheen tuotteita. Näistä esimerkiksi Teams-viestintäjärjestelmää koulutettiin vuoden 2019 syksystä lähtien ja tiedotusta niin tiimeissä kuin koko yrityksessä oli aloiteltu kyseisen välineen avulla. Myös tiimien keskinäinen keskustelu saatiin käynnistymään em. koulutusten kautta. Kohdeyritys suoritti tietämättään tiedon jakoa yhdessä toimien, teoriassa puhutaan tästä mm. sanoin Wisdom of Crowds sekä joukkouttaminen (Hyyppä, 2019). O365-perheen lomakesovelluksena toimii Forms. Perehdytyskulttuurin kehittämistarpeiden selvittämiseksi tuli saada selville kohdeyrityksen henkilökunnan ymmärrys tietoturvasta. Tähän liittyen tehtiin henkilöstölle ensin kyselytutkimus tietoturvasta, johon asetettiin mukaan perustavanlaatuisia kysymyksiä. Samalla mahdollistettiin loppukäyttäjien omien huolien esiintuonti. Forms ’iin tehty kysely kehitettiin yhteistyössä tietohallinnon tiimin kanssa, jotta kyselyyn saatiin mukaan asioita, joiden avulla saadaan myös tarkoituksenmukaisia vastauksia. Tulokset tästä kyselystä on esitetty kappaleessa 4.1.1. Näiden tulosten pohjalta päätettiin lähestyä käyttäjien perehdytysmenetelmiä selvittämällä heille paras oppimismekanismi. Tämän havainnollistamiseksi suoritettiin uusi Forms -kysely oppimisesta. Mekanismin selvittämisessä käytettiin mallina yrityksessä käytössä ollutta LABS-kyselymekanismia, jossa eri ryhmille perehdytettiin tietoturvaa neljällä erilaisella tavalla. Tästä saatiin tulokseksi, että ajankäytöllisesti ja asiasisällöllisesti parhaat tulokset perehdytyksen onnistumisesta saadaan esittämällä aihepiirin materiaali videoin ja nasevin tekstein. Videomateriaali hankittiin yrityksen ulkopuolelta. O365-perheen muista tuotteista tietohallinnon tiimi tutustui Stream-sovellukseen. Kyseisen sovelluksen avulla tuotettiin kohdeyritykselle tietoturvaperehdytyksen uusi materiaali, joka koostui pääasiassa 2-3 aihepiirin videosta ja joka jaettiin ympärivuotiseen käyttöön, kappaleen 4.3. mukaisesti. Vuosikello on merkityksellinen apuväline myös Valtiovarainministeriön vuosisuunnittelussa sekä -seurannassa (Valtiovarainministeriö, 2016), joka toimii yhtenä kohdeyrityksen ohjaajana.

Valitut kysely- ja perehdytysmekanismit sekä O365-perheen tuotteiden käyttöönotto tukevat yrityksen kehittymistavoitteita sekä perehdyttävät henkilöstöä lähes automaattisesti paitsi tietoturvaan, myös työvälineisiin (Jansson, 2019b). Alkuvuoden 2020 aikana kyseiset välineet ovatkin jokapäiväisessä käytössä. Tietoturvaperehdytyksissä käytettävä aineisto on henkilöstön käytettävissä myös etätöissä tai omalta koneelta, ajasta ja paikasta riippumatta. Näin ollen aineistoon perehtymisen voi suorittaa parhaiten omaan ajankäyttöön soveltuvana aikana, jolloin se

palvelee parhaiten oppimista. Kohdeyrityksen tietoturvan perehdytyskulttuuria on aiemmin mainittujen välineiden avulla pystytty kehittämään suurin askelin. Materiaalin ollessa helpposelkoista ja sen ollessa jaettuna riittävän pieniin kokonaisuuksiin, on siitä luotu hyvin ymmärrettävä ja sisäistettävä kokonaisuus. Näin ollen on onnistuttu muuttamaan perehdytyskulttuuria esimerkiksi Emma O'Neillin (O'Neil Emma, 2019) sekä Susanna Järvilehdon ja Kaisa Leinon (Järvilehto and Leino, 2019) malleja mukaillen. Näin myös tiedon jalkauttaminen sekä ajankäyttö on oleellisesti helpottunut, niin kuulijan kuin kertojan osalta.

Tietoturvan perehdyttämisen tulee ulottua koko henkilöstöön, sidosryhmiin ja ulkopuolisiin toimijoihin (Pori Energia Oy Johtoryhmä, 2019). Näin ollen perehdytykset tulee ulottaa myös erilaisiin harjoittelijoihin, opiskelijoihin sekä kesätyöntekijöihin eli periaatteessa kaikkiin, jotka jollain tavalla tulevat toimimaan kohdeyrityksen toimintaympäristössä. Tästä syystä työn kohteena on paitsi vakituinen henkilökunta, myös lyhyempiaikaisten toimijoiden oma tietoturvallisuuden perehdytysohjelma. Lisäksi henkilöstöhallinnon perehdytyssuunnitelmaan tulee lisätä erityisesti tietoturvaperehdytyksen läpikäynti. Kaikkiin perehdytyksiin tehdään oma kysymysosuus, joka tulee täyttää suoritettuaan kyseisen osuuden. Tämä koskee sekä ympärivuotisia perehdytyksiä kuin perehdytysjaksoja suorittavia henkilöitä.

5.2 Päätulokset

Työn aikana suoritettu analysointi nykymenetelmien toimivuudesta ja riittävyydestä tietoturvan perehdytysmenetelmänä kertoi, että olemassa olevan aineiston sisältö on kattava, kouluttajan tapa perehdyttää on miellyttävä ja kertova, mutta kokonaisuus on aikaa vievä, molemmin puolin. Samalla voidaan todeta, että aineiston itsenäinen läpikäynti jättää perehdytykseen selkeitä aukkoja, koska osassa materiaalia tarvitaan aina kertojaa. Yritys tarvitsee ehdottomasti uutta perehdytyskulttuuria tälle alueelle.

Tehtyjen tutkimusten, testausten, kyselyiden ja pilotointien perusteella yrityksen henkilökunta on valmis ottamaan vastaan nykyaikaisia ja tehokkaita perehdytysmenetelmiä. Materiaalin riittävän pieni annostelu, pituus ja motivoivuus antavat koulutettavalle enemmän ja lyhyemmässä ajassa kuin perinteiset perehdytyskeinot. Koska oppiminen on jatkuvaa, suosittelen innostamaan henkilökuntaa käyttämään nykyistä laajemmin O365-sovelluksia, erityisesti tiedonjakoa ja keskusteluun kannustavaa Teams'iä sekä kohdeyrityksen kouluttavia ja informoivia Stream -videoita. Lisäperehdytykset näille alueille ovat suositeltavia, jotta sovellusten käyttö on sujuvaa.

Edellä mainituista välineistä koostuva perehdytysaineisto kannattaa julkaista yrityksen Stream -sovelluksessa Tietoturva -kanavalla, josta se on koko henkilökunnan katsottavissa. Suunniteltu tietoturvan perehdytysohjelma sekä koulutuksen ajallinen vuosikello kannattaa tehdä seuraavaksi kahdeksi (2) vuodeksi. Vuosikellon tehtävänä on jaksottaa tietohallinnon toimet tasaisesti, toisiaan tukien, pitkin vuotta sekä samalla huomioida kohdeyrityksen tietohallinnon muut ajastettavat toiminnot. Vuosikellon hyödyntäminen mm. julkaisuaikatauluissa saattaisi olla hyvä keino kannustaa ihmisiä "odottamaan" uutta materiaalia. Tehdyt testit perehdytyksen jälkeen voivat käynnistää mittarien käytön myös koulutuksellisesta aspektista ja innostaa lisäkoulutuksiin.

5.3 Jatkokehitysehdotukset

Työn valmistuttua kannattaa välittömästi aloittaa kulttuurin varsinainen jalkautus. Jalkautuksen onnistumista pitää jollain tasolla analysoida ja pyrkiä kehittämään menetelmää pidemmälle. Mietittäväksi kannattaa ottaa myös nyt suositellun tavan eteenpäin vienti, esimerkiksi luomalla omia perehdytysvideoita ostettujen oheen ja saada näin kohdeyrityksen omaa ääntä kuuluville. Tämänhetkiset tietoturvatarinat kouluttajan kertomina ovat olleet innostavia ja herättäviä, jolloin niiden käyttö jatkossakin olisi suositeltavaa. Tietoturvan jalkautuksen ylläpitämiseksi ja kehittymistä ajatellen vuosikellon hyödyntäminen kohdeyrityksessä pitää jalkautuksen jatkuvasti mukana suunnitelmissa ja sitä kautta ajankohtaisena. Alustava suunta kehityksessä on pelillistämisen mukaanotto vuosikello -suunnitteluun. Innostus tietoturvaan liittyvien pelien käyttöönottoon yrityksissä kasvaakin koko ajan. Tietoturvaperehdytyskulttuurin luomisessa ja sen kehittämisessä jatkossa kannattaakin ottaa huomioon pelillistäminen, erilaiset kilpailut sekä palkitseminen. Pelien vahvuus on siinä, että ne saavat helpommin ihmisen motivoituneeksi ollessaan kilpailuhenkisiä. Pelillä on ns. koukuttava ominaisuus, mikäli se on hyvin suunniteltu ja kohdistettu ja se on samalla hauska. Taktiset ja simulaatiota käyttävät pelit opettavat pelin aikana ihmisten aivoja (Lappalainen, 2017). Pelistä saa myös usein palkinnon, vaikka virtuaalisenkin, joten se kiinnostaa. CGI on 27.11.2019 julkaissut yhteistyössä Liikenne- ja viestintävirasto Traficomin sekä Valtion kehitysyhtiö Vaken kanssa alakoululaisille suunnatun tietoturvaan perehdyttävän pelin, joka opettaa suojautumaan nettikiusaamiselta ja huijausviesteiltä. Lisäksi se opettaa käyttäjiään pelinomaisella tavalla salasanojen, yksityisyyden sekä netin käytöstapojen perustaitoihin. Nuorille ja alakoululaisille suunnattu peli perustuu lasten kyberturvallisuuden ymmärryksen parantamiseen ja kehittämiseen. Pelin avulla heillä on mahdollisuus oppia turvallista netin käyttöä ja suojautumista digiturvallisuuden uhkia vastaan.(Nikko-Takala, 2019). Työssä onkin mietitty pelillistämisen mukaan ottoa vuosisuunnitteluun ja sitä kautta kehittää tietoturvallisuuskulttuuria pidemmälle. Pelien tuominen yritysympäristöön voi alkuun olla haaste, mutta huolellisella suunnittelulla ja pilotoinnilla, innovatiivisella ja motivoituneella käyttäjäkunnalla päästään hyviin tuloksiin. Vuoden 2021 lopun aikana siirtyminen videoperehdytyksistä pelillisiin perehdytyksiin tulee olemaan haaste, mutta tuloksia tuottava.

Kybersään seuraaminen on pidettävä säännöllisenä niin yrityksen johdon toimesta kuin jokaisen henkilökunnan jäsenen saatavilla helposti. Kybersää voidaan liittää perehdytysmateriaalin itsemuokattaviin osiin vuosikellon mukaisessa aikataulussa. Suositeltaviin toimenpiteisiin kuuluu ehdottomasti ensimmäisen Tietoturvakyselyn tuloksissa nähtävä salasanojen runsaus ja tapa pitää niitä muistissa. Tähän suosittelen voimakkaasti salasanasovelluksen käyttöönottoa keskitetysti koko yrityksessä niin työasemiin kuin mobiililaitteisiin, helpottamaan työn sujuvuutta sekä tietoturvaa.

Muutokset kulunvalvonnan ohjeistuksissa tehtiin syksyllä 2019, jolloin muutettiin kulunvalvontaan liittyviä ohjeita siten, että kaikilla yrityksen työntekijöillä tulee olla henkilökortti selkeästi näkyvillä. Kulunvalvonnan ohjeita on myös otettu mukaan uuteen perehdytysmateriaaliin, jotta kaikilla henkilökunnan jäsenillä on esimerkiksi tieto, miten pitää toimia vieraiden kanssa yrityksen toimitiloissa. Huhtikuussa 2020 ollaan, aiempien ohjeiden lisäksi, ottamassa käyttöön uutta vierailijakorttimekanismia yrityksen päätoimipaikassa. Näin voidaan varmistaa, että vierailulle tulleet henkilöt ovat rekisteröityneet yritykseen asianmukaisesti.

Vuosi 2020 tulee olemaan merkityksellinen vuosi kohdeyrityksen historiassa eikä vähiten sen vuoksi, miten se Korona -pandemian aikana toimii kriisitilanteessa, vaan siksi, että vuosi 2020 on tietoturvallisuuden uusi vuosi perehdytysohjelmineen ja teknisine muutoksineen koko yrityksessä.

LÄHTEET

2NS - Second Nature Security (2019) *Tietoturvakoulutus henkilöstölle*, *Kyberoppi-verkkokoulutus*. Available at: https://www.2ns.fi/palvelut/koulutus/ (Accessed: 1 October 2019).

Ahponen, P. (1997) *Riskikirja: Uhat, mahdollisuudet ja asiantuntijuus epävarmuuden yhteiskunnassa*. Jyväskylä: Jyväskylän Yliopisto.

Business Technology Standard (2020) *Kokonaisarkkitehtuuri*.

Casual Learning (2020) 'Bake the world a better place', *Casual Learning*, (Recipes to address new target groups with development education). Available at: http://www.bakeabetterplace.org/methods - kitchen tools/CASUAL LEARNING/Casual lerning more.html.

Chanal, V. and Caron-Fasan, M.-L. . (2010) *The Difficulties involved in Developing Business Models open to Innovation Communities: the Case of a Crowdsourcing Platform.* Available at: https://fi.wikipedia.org/wiki/Joukkouttaminen.

Contrasec Oy (2019) *IT-palvelut yrityksellenne*, *Organisaation tietoturva*. Available at: https://contrasec.fi/kurssi/organisaation-tietoturva/ (Accessed: 22 August 2019).

Digimoguli Oy (2019) 'Markkinoinnin vuosikello 2020', *Digimoguli*, (Vuosikello). Available at: https://digimoguli.fi/blogi/markkinoinnin-vuosikellon-luominen-ilmainen-pohja/.

European parliament and Council (2016) *The Directive on security of network and information systems (NIS Directive)*, *Directive (EU) 2016/1148 of the European Parliament and of the Council*. Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Finlex and Oikeusministeriö (1999) *Laki viranomaisten toiminnan julkisuudesta*. Suomi. Available at: https://www.finlex.fi/fi/laki/alkup/2019/20190906.

Finlex and Oikeusministeriö (2011) *Valmiuslaki*. Suomi. Available at: https://www.finlex.fi/fi/laki/ajantasa/2011/20111552.

Finlex and Oikeusministeriö (2018) *Tietosuojalaki*. Suomi. Available at: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.

Finlex and Työ- ja elinkeinoministeriö (2013) *Sähkömarkkinalaki*. Suomi: Työ- ja elinkeinoministeriö. Available at: https://www.finlex.fi/fi/laki/ajantasa/2013/20130588?search%5Btype%5D=pika&search%5Bpika%5D=Tietoturva.

Finlex and Valtiovarainministeriö (2019) *Tiedonhallintalaki - Laki julkisen hallinnon tiedonhallinnasta*. direktiivi 2013/37/EU. Available at: https://www.finlex.fi/fi/laki/smur/2019/20190906.

Granite Partners (2019) *Tietoturvakoulutus verkossa Turvaa menestyksesi koulutuksella*. Granite Partners. Available at: https://granite.fi/tietoturvakoulutus/ (Accessed: 8 August 2019).

Hakala, M., Wuorinen, O. and Vainio, M. (2006) *Tietoturvallisuuden käsikirja*. Jyväskylä: Docendo.

Henkilöstöhallinto (2020) *Perehdytyssuunnitelma*. Pori. Available at: m-

files://show/F65E8929-BEFF-4A06-9A10-8A52F9325A55/0-56794?object=8A59EBBC-2F3C-4B8E-BF19-08ECF6616F17.

Huhtanen, A. (2017) *Oppiminen, mitä se oikeastaan on?*, *Dare to Learn*. Available at: http://www.daretolearn.fi/blog/mita-on-oppiminen-tarkemmin-ajatellen#.

Hyyppä, H. (2019) 'Yhteisöllisyys – pikkuasioita ja kokonaisuuksia', *Psykoterapia*, 02, pp. 176–177. Available at: http://www.psykoterapia-lehti.fi/tekstit/psyk_022019_hyyppa.pdf.

ICT Standard Forum (2019a) *IT-johtamisen kansainväliset mallit ja standardit*. Available at: https://www.itforbusiness.org/fi/book/tyokalut-standardit/it-johtamisen-kansainvaliset-mallit-ja-standardit/.

ICT Standard Forum (2019b) *IT Standard for Business - Tietoturva, riskienhallinta ja laadunvarmistus*. Available at: https://www.itforbusiness.org/fi/book/strategia-ja-hallinto/tietoturva-riskienhallinta-ja-laadunvarmistus/.

ICT Standard Forum (2019c) *IT Standard for Business – a Model for Business driven IT Management*. Available at: https://www.itforbusiness.org/fi/book/strategia-ja-hallinto/julkinen-hallinto/.

Jansson, J. (2019a) *Esitysmateriaali - ICT-Jory 15.2.2019*. Pori.

Jansson, J. (2019b) 'Haastattelu tietojärjestelmistä ja salasanamekanismeista'. Pori: Pori Energia, pp. 16–17.

Jansson, J. (2019c) *Perehdytys tietoturvaan -esitysmateriaali*. Available at: m-files://show/F65E8929-BEFF-4A06-9A10-8A52F9325A55/0-103990?object=4C700195-9913-46BA-BA08-AF016B39A5CB.

Järvilehto, L. (2019) *Palikkamallista aaltomalliin*, *PALIKKAMALLISTA AALTOMALLIIN*.

Järvilehto, S. and Leino, K. (2019) *Väitämme: Jatkuva oppiminen on aikamme tärkein kilpailuvaltti*. Helsinki. Available at: https://www.paperplanes.fi/blogi/vaitamme-jatkuva-oppiminen-on-aikamme-tarkein-kilpailuvaltti/.

Jokinen, S. (2019) *Mitä jokaisen toimitusjohtajan tulee tietää tietoturvasta?*, *Triuvare*. Available at: https://materiaalit.triuvare.fi/artikkelit/mita-jokaisen-toimitusjohtajan-tulee-tietaa-tietoturvasta?utm_medium=ppc&utm_campaign=Triuvare&utm_term=tietoturva&utm_source=adwords&hsa_ad=388390387612&hsa_kw=tietoturva&hsa_cam=44516759&hsa_src=g&hsa_tgt=kwd-2 (Accessed: 24 September 2019).

Kankaanpään Yhteislyseo (2019) *Oppiminen ja opiskelutekniikat*, *Peda.net*. Available at: https://peda.net/kankaanpää/ky/oppiaineet/opinto-ohjaus/ojo (Accessed: 2 January 2020).

Kansainvälinen Kauppakamari (2019) *Tietoturvaopas yrityksille - ICC Cyber security guide for business*. 450/1081–5. Edited by Keskuskauppakamari. Kansainvälinen kauppakamari.

Kaukosalmi, R. (2019) 'Office 365-pilvipalvelu käyttöön syksyllä - miten se vaikuttaa työskentelyyn?', *Voimavara*, 550, p. 16.

Kielitoimisto (2020) *Kielitoimiston sanakirja*, *Kotimaisten kielten keskus ja Kielikone Oy*.

Koivukunnas, A. (2018) 'Miten ihminen oppii', *Hevosilo*, (Kohtaamisia hevosen ehdoilla).

Koivula, E. (2019) *MIKSEI VIDEOIDEN TEKEMINEN NAPPAA – 4 ERILAISTA IHMISTYYPPIÄ*, *Tiski*.

Laaksonen, M., Nevasalo, T. and Tomula, K. (2006) *Yrityksen tietoturvakäsikirja : ohjeistus, toteutus ja lainsäädäntö*. Helsinki: Edita.

Lappalainen, E. (2017) ‘Perinteinen tietoturvakoulutus ei toimi’, *Tivi*, (Digitalous). Available at: https://www.tivi.fi/uutiset/f-securen-hypposen-uusi-projekti-perinteinen-tietoturvakoulutus-ei-toimi/8b89aadf-c98a-3087-a4bc-004d22cb14a4.

Lavonen, J. and Meisalo, V. (2003) *TYÖTAPAOPAS - YHTEISTOIMINNALLISET TYÖTAVAT*. Helsinki. Available at: http://www.edu.helsinki.fi/malu/kirjasto/yto/yto/.

Leino, K. (2019a) *Näin teet koukuttavia opetussisältöjä – 10+1 vinkkiä*. Helsinki. Available at: https://www.paperplanes.fi/blogi/nain-teet-koukuttavia-opetussisaltoja/.

Leino, K. (2019b) *Näin teet koukuttavia opetussisältöjä – 10+1 vinkkiä*, *Paperplanes*.

Manninen, O., Suomala, P. and Lyly-Yrjänäinen, J. (2018) *Laskentatoimi johtamisen tukena*. Available at: www.editapublishing.fi/oppimateriaalit/tuote/laskentatoimi-johtamisen-tukena.

Markkinointi, P. E. O. (2018) *Pori Energia Oy*. Available at: www.porienergia.fi (Accessed: 25 July 2018).

Microsoft (2020) *Universaali ympäristö käyttäjätietojen hallintaan ja suojaamiseen*. Available at: https://www.microsoft.com/fi-fi/windows/windows-hello (Accessed: 2 January 2020).

Niemi, T. (Pori E. O. (2020) ‘Haastattelu LABS-mekanismista Pori Energia Oy:ssä’. Pori.

Nikko-Takala, P. (2019) *Alakoululaiset saavat mobiilipelin digiturvataitojensa treenaamiseen*, *CGI Tietopankki*. Available at: https://www.cgi.fi/fi/uutiset/alakoululaiset-saavat-mobiilipelin-digiturvataitojensa-treenaamiseen (Accessed: 27 November 2019).

NIST (2019) *CYBERSECURITY*. Available at: https://www.nist.gov/topics/cybersecurity (Accessed: 1 August 2019).

Nygren, J. (Prisma S. (2015) *Väärinkäsitys: Jokaisella on oma oppimistyylinsä*. Suomi: Prisma Yle Areena. Available at: https://yle.fi/aihe/artikkeli/2015/07/16/vaarinkasitys-jokaisella-oma-oppimistyylinsa.

O’Neil Emma (2019) *20 Tips for Creating a Learning Culture in the Workplace*, *LearnUpon*. Available at: https://www.learnupon.com/blog/learning-culture/ (Accessed: 1 February 2020).

Oikeusministeriö (1999) *Julkisuuslaki, Laki viranomaisten toiminnan julkisuudesta*.

Oikeusministeriö (2019) *Tietosuojalaki 1050/2018, 6§*. Available at: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050#L5P27.

Oikeusministeriö (2020) ‘Suomen Perustuslaki’. Helsinki. Available at: https://www.finlex.fi/fi/laki/ajantasa/1999/19990731.

Pfleeger, C. P., Pfleeger, S. L. and Margulies, J. (2003) *Security in Computing*. 5th edn. Westford, Massachusetts.

Plandisc (2020) *Vuosikellotyökalu sujuvaan suunnitteluun*, *Plandisc*. Available at: https://plandisc.com/fi/?gclid=CjwKCAjw3-bzBRBhEiwAgnnLCriS-S7w9T0e7pjcl3xfIwOfDJkNyV9KaKwgyg-RStm4Atfz0NA0PhoC8FQQAvD_BwE (Accessed: 24 March 2020).

Pori Energia Oy (2019) *Pori Energia toimintakertomus 2019*. Pori. Available at: https://www.porienergia.fi/yritys/vuosikertomus#.XpMZj_gzZnI.

Pori Energia Oy henkilöstö (2020) *Pori Energia Oy konsernin Arvot*, *www.porienergia.fi*. Available at: https://www.porienergia.fi/yritys#.XpM0rPgzZnI (Accessed: 12 April 2020).

Pori Energia Oy Johtoryhmä (2019) *ICT-tietoturvapolitiikka*. Pori.

Ristolainen, M. (2020) ‘Haastattelu koulutuksista kohdeyrityksessä’. Pori.

Ruonala, K. (2011) *KUNNAN TIETOTURVAJOHTAMINEN – TIETOTURVAN JALKAUTTAMINEN OSAKSI ARKIPÄIVÄN TOIMINTAA*. Rovaniemi. Available at: https://www.theseus.fi/bitstream/handle/10024/30571/Ruonala_Keijo.pdf?sequence=1&isAllowed=y.

Sheng Kung *et al.* (2012) *The Wisdom of the Crowd in Combinatorial Problems*. doi: 10.1111/j.1551-6709.2011.01223.x.

Teosto (2018) 'Tietoturvapolitiikka', *Teosto*. Teosto. Available at: https://www.teosto.fi/teosto/artikkelit/tietoturvapolitiikka.

Traficom (2020) *Kybersää*, *Kyberturvallisuuskeskuksen julkaisu*. Available at: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa (Accessed: 29 March 2020).

Tuomola, R., Maijanen, A. and Prashnig, B. (1999a) *Opetusmenetelmät opetuksen monipuolistajana*. Oulu. Available at: http://www.oamk.fi/amok/oppimat/LO/Opetusmenetelmat06a/html/johdanto.html.

Tuomola, R., Maijanen, A. and Prashnig, B. (1999b) *Opetusmenetelmät opetuksen monipuolistajana*. Oulu. Available at: http://www.oamk.fi/amok/oppimat/LO/Opetusmenetelmat06a/html/johdanto.html.

Työ- ja elinkeinoministeriö (2014) *Laki Energiavirastosta*. Available at: http://www.finlex.fi/fi/laki/ajantasa/2013/20130870.

Useita (2018) *Joukkouttaminen*, *Wikipedia*. Available at: https://fi.wikipedia.org/wiki/Joukkouttaminen (Accessed: 6 January 2020).

Vähänen-Koivuluoma, T. (2018) *PIELEEN MENI! PIENYRITYKSIEN YRITYSRISKIEN HALLINTAMENETELMIEN KEHITTÄMISESTÄ*. Pori.

Valtiohallinnon tietoturvallisuuden johtoryhmä (2001a) *5.3 Järjestelmien hallintaan liittyvät riskit*. Available at: https://www.vahtiohje.fi/web/guest/riskienhallinta;jsessionid=B0CF6DCEB2EFD8686C2E7D6638935230A47387766F60009AA82F13712A646E54D45F658B8D26FA623829A3.

Valtiohallinnon tietoturvallisuuden johtoryhmä (2001b) *Riskienhallinta, Vahti 5/2001*. Helsinki. Available at: https://www.vahtiohje.fi/web/guest/riskienhallinta.

Valtiohallinnon tietoturvallisuuden johtoryhmä (2013) 'Henkilöstön tietoturvaohje, Vahti 4/2013', in *VAHTI 4/2013*. Helsinki: Juvenes Print - Suomen Yliopistopaino Oyj, p. 17. Available at: https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229.

Valtionvarainministeriö (2009) *VAHTI: Tilannetietoisuus ja riskienhallinta*. Helsinki.

Valtiovarainministeriö (2009a) *Lokiohje*. Helsinki: Pirkko Ala-Marttila/VM-julkaisutiimi.

Valtiovarainministeriö (2009b) *VAHTI -ohjeet*. Helsinki.

Valtiovarainministeriö (2016) 'Jatkuvuuden hallinnan vuosikello (esimerkki)', *VAHTI 2/2016*. Valtiovarainministeriö, Vahti 2/2016. Available at: https://www.vahtiohje.fi/web/guest/774.

Venhe, N. (2018) *Tekniikka antaa välineitä yksilöllisempään opetukseen*. Joensuu ja Kuopio. Available at: https://www.uef.fi/-/tekniikka-antaa-valineita-yksilollisempaan-opetukseen.

Vuorinen, I. (2001) *Opetusmenetelmät opetuksen monipuolistajana, esittävä opetus*. Oulu. Available at: http://www.oamk.fi/amok/oppimat/LO/Opetusmenetelmat06a/html/esittava_op_.html.

LIITE A

Otteita energiayhtiöitä koskevien lakien ja asetusten sisällöstä

Energiayhtiöitä koskevat lait ja säädökset säätelevät niin muiden kuin kohdeyrityksen toimintaa. Ohessa olevat otteet lakikohdista kertovat, miten lakipykälät viittaavat tietoturvallisuuteen, jota yrityksissä tulee noudattaa.

Perustuslaki

29a§ Sähkömarkkinalaki:

”Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen

Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa.”

(Oikeusministeriö, 2020)

66§ Sähköntoimittajan sopimustietojen säilyttäminen

”Sähköntoimittajan on säilytettävä merkitykselliset tiedot kaikista sähköntoimitussopimuksiin liittyvistä liiketoimistaan ja suuntaviivoja koskevassa Euroopan komission asetuksessa tai päätöksessä säädetyt tiedot sähköjohdannaisiin liittyvistä liiketoimistaan tukkuasiakkaiden ja kantaverkonhaltijoiden kanssa vähintään viiden vuoden ajan sen tilikauden päättymisestä, jonka kuluessa liiketoimi on suoritettu. Säilytettäviä tietoja ovat ainakin:

1) liiketoimen kesto;

2) toimitukseen ja selvitykseen liittyvät menettelytavat;

3) toimituksen määrä;

4) toteutusaika;

5) hinta;

6) sopijapuolen yksilöivät tiedot;

7) tiedot selvittämättä jääneistä sopimuksista.”

(Oikeusministeriö, 2020)

75 c § (18.1.2019/108) Sähkökaupan markkinaprosesseihin liittyvän tiedon säilyttäminen

”Sähköalan yrityksen on säilytettävä tässä laissa säädettyjä, sähkökaupan keskitetyn tiedonvaihdon palveluihin, sähkökaupan markkinaprosesseihin, tasevastuun täyttämiseen ja taseselvitykseen liittyviä tehtäviä tai velvollisuuksia suorittaessaan tai täyttäessään saamansa tiedot kuuden vuoden ajan tapahtumasta, jota tieto koskee tai, jos kysymyksessä on sopimusta koskeva tieto, kuuden vuoden ajan sopimuksen päättymisestä. Henkilötiedot on poistettava sähköalan yrityksen rekisteristä tämän ajan päätyttyä, ellei niiden käsittelyyn tämän ajan jälkeen ole muuta oikeusperustetta.”

(Oikeusministeriö, 2020)

76 § (18.1.2019/108) Salassapitovelvollisuus ja hyväksikäyttökielto

”Sähköalan yritys on velvollinen pitämään salassa tässä laissa, sähkökauppa-asetuksessa tai energian tukkumarkkinoiden eheydestä ja tarkasteltavuudesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 1227/2011 tarkoitettuja tehtäviä suorittaessaan tietoonsa saamansa asiakkaansa tai muun verkon käyttäjän liikesalaisuuden, jollei tiedon ilmaiseminen toiselle perustu tässä laissa tai mainituissa asetuksissa säädettyyn oikeuteen tai se, jonka hyväksi vaitiolovelvollisuus on säädetty, anna suostumustaan sen ilmaisemiseen.

Sähköalan yritys on velvollinen pitämään salassa tässä laissa tai sähkökauppa-asetuksessa tarkoitettuja tehtäviä suorittaessaan tietoonsa saamansa tiedon, joka koskee:

1) maanpuolustusta palvelevia rakenteita, laitteita tai järjestelmiä, maanpuolustuksen kannalta muutoin merkityksellisiä kohteita tai puolustusvalmiuteen varautumista, jollei ole ilmeistä, että tiedon ilmaiseminen ei vahingoita eikä vaaranna maanpuolustuksen etua;

2) poikkeusoloihin varautumista tai väestönsuojelua, jos tiedon ilmaiseminen vahingoittaisi tai vaarantaisi turvallisuutta tai sen kehittämistä, väestönsuojelun toteuttamista tai poikkeusoloihin varautumista;

3) tieto- ja viestintäjärjestelmiin kuuluvia rakenteita, laitteita tai kohteita tai tieto- ja viestintäjärjestelmien turvajärjestelyjä, jollei ole ilmeistä, että tiedon ilmaiseminen ei vaaranna tieto- ja viestintäjärjestelmien turvajärjestelyjen toteutumista.

Salassa pidettäviä tietoja ei saa antaa myöskään yhtiökokoukselle, osuuskunnan kokoukselle tai edustajistolle eikä kokoukseen osallistuvalle osakkeenomistajalle tai jäsenelle. Salassapitovelvollisuus koskee myös sähköalan yrityksen toimielimen jäsentä ja varajäsentä ja sen palveluksessa tai toimeksiannosta työskentelevää henkilöä, joka tässä pykälässä tarkoitettuja tehtäviä suorittaessaan on saanut tietää salassa pidettävän seikan.

Sähköalan yrityksellä on kuitenkin velvollisuus antaa 1 momentissa tarkoitettuja tietoja viranomaiselle, jolla on lain mukaan oikeus niitä saada.

Sähköalan yritys ja tässä pykälässä tarkoitettu henkilö eivät saa käyttää salassapitovelvollisuuden piiriin kuuluvia tietoja omaksi hyödykseen eivätkä toisen hyödyksi tai vahingoksi.”

(Finlex and Työ- ja elinkeinoministeriö, 2013)

Laki viranomaisen toiminnan julkisuudesta (Finlex and Oikeusministeriö, 1999) sekä valmiuslaki (Finlex and Oikeusministeriö, 2011)

”1 § Lain tarkoitus

Tämän lain tarkoituksena on poikkeusoloissa suojata väestöä sekä turvata sen toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys.

2 § Soveltamisala

Tässä laissa säädetään viranomaisten toimivaltuuksista poikkeusolojen aikana. Lisäksi laissa säädetään viranomaisten varautumisesta poikkeusoloihin.

3 § Poikkeusolojen määritelmä

Poikkeusoloja tämän lain mukaan ovat:

1) Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila;

2) Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii tämän lain mukaisten toimivaltuuksien välitöntä käyttöön ottamista;

3) väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat;

4) erityisen vakava suuronnettomuus ja sen välitön jälkitila; sekä

5) vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti.”

(Finlex and Oikeusministeriö, 2011)

Tietohallintolaki (Finlex and Valtiovarainministeriö, 2019)

”1§ Lain tarkoitus

Tämän lain tarkoituksena on tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta säätämällä julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteentoimivuuden edistämisestä ja varmistamisesta.

Viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) tarkoitetusta valtion viranomaisen tietoturvasta ja valmiuslaissa (1080/1991) tarkoitetusta valtion viranomaisen poikkeusoloihin varautumisesta on tietohallinnossa voimassa, mitä niistä säädetään mainituissa laeissa.”

Tietosuojalaki (Finlex and Oikeusministeriö, 2018)